Рівненський державний гуманітарний університет
Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин

Методичні рекомендації до семінарських занять з дисципліни «Інформаційна безпека»

для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності
291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

Рівне-2023 рік

УДК 351.746:007(072)
М 54
Методичні рекомендації до семінарських занять з дисципліни «Інформаційна безпека» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Рівне: РДГУ, 2023. 38 с.

Розробник: к.політ. наук, доц. кафедри міжнародних відносин **Кундеус О. М.**

Рецензенти:

Вівчар І.В. кандидат політичних наук, доцент кафедри міжнародних відносин РДГУ.

Чернюк І.А. кандидат політичних наук, доцент кафедри суспільних наук Національного університету водного господарства та природокористування.

Методичні рекомендації до семінарських занять складаються з вказівок до вивчення дисципліни, які разом з лекційним курсом допоможуть студентам більш глибоко зрозуміти та засвоїти зміст дисципліни «Інформаційна безпека». Також методичні вказівки містять плани семінарських занять, тематику індивідуальних завдань та контрольних робіт, питання модульного та підсумкового контролю, термінологічний словник, список рекомендованої літератури.

Затверджено на засіданні кафедри міжнародних відносин
Протокол від 30 серпня 2023 № 8

Завідувач кафедри
міжнародних відносин _____ **(доц.. Крет Р.М.)**

Схвалено науково-методичною радою факультету історії, політології та міжнародних відносин
Протокол від.31 серпня 2023р. № 7

Голова методичної ради _____ **(проф.. Галуха Л.Ю..)**

Зміст

1. Опис навчальної дисципліни.

2. Мета й завдання дисципліни, її місце у навчальному процесі.

2.1. Мета викладання дисципліни.

2.2. Завдання вивчення дисципліни. Знання та вміння студентів.

2.3. Міждисциплінарні зв'язки.

2.4. Форми контролю знань і критерії оцінювання з курсу.

3. Структура та зміст дисципліни.

3.1. Тематика та зміст практичних (семінарських) занять

3.2. Методичні рекомендації з підготовки практичних (семінарських) занять.

4. Самостійна робота студентів.

4.1. Мета й завдання самостійної роботи студентів.

4.2. Форми організації самостійної роботи.

4.3.Методичні рекомендації до самостійної роботи.

4.4. Перелік питань для самостійної роботи.

4.5.Методичні поради до написання реферату.

4.6. Індивідуальні завдання (теми рефератів).

5. Методичні рекомендації для виконання контрольних робіт.

5.1.Питання на контрольну роботу.

6. Питання на іспит.

7. Термінологічний мінімум.

8. Список рекомендованої літератури.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів –4</td><td>Галузь знань:
29 міжнародні відносини</td><td>Обов’язкова</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність
Міжнародні відносини, суспільні комунікації та регіональні студії.</td><td>Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання _____</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин - 120</td><td>1-й</td></tr>
<tr><td></td><td>Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: 2
аудиторних – 2
самостійної роботи студента - 50</td><td rowspan="10">Освітньо-кваліфікаційний рівень:
Бакалавр</td><td>20 год.</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>28 год.год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72год.</td></tr>
<tr><td>Індивідуальні завдання: год.</td></tr>
<tr><td>Вид контролю:
іспит</td></tr>
</table>

2. Мета й завдання дисципліни, її місце в навчальному процесі

2.1. Мета викладання дисципліни

Інформаційні системи все більше ускладнюються, взаємозалежність між різноманітними компонентами вже не завжди очевидна, тому інформаційна безпека й політика набувають все більш глобального характеру, виходячи в більшості випадків на перший план.

XXI ст. перед суспільством із погляду безпеки поставило цілу низку нових проблем. Процеси глобалізації дуже гостро дали про себе знати й, окрім позитивних елементів, виникли серйозні негативні явища, до яких світова спільнота виявилася не готовою.

Явища глобалізаційного характеру в інформаційній та телекомунікаційній сферах дуже гостро поставили питання про охорону національної самоідентичності, оскільки в цьому аспекті є величезна загроза. Виходячи з правового аналізу інформаційного законодавства України, інформаційна безпека виступає одним із багатьох його провідних багатоаспектних чинників (об'єктом правовідносин).

Інформаційна безпека – комплексна дисципліна, вивчення якої спрямоване на формування у студентів системного підходу до вирішення завдань практичного, прикладного характеру в умовах викликів інформаційного суспільства і продуктивного існування в побутових і виробничих умовах та за екстремальних обставин.

Дисципліна «Інформаційна безпека» підготовлена для студентів спеціальності «Міжнародні відносини, суспільні комунікації та регіональні студії».

Курс передбачає вивчення студентами особливостей формування державної інформаційної політики та пов'язаних із цим питань охорони інформаційного простору України як чинника національної безпеки.

2.2. Завдання вивчення дисципліни. Знання та вміння студентів

Завдання вивчення дисципліни:

✓ ознайомити студентів із визначенням та класифікацією національної безпеки;

✓ визначити поняття інформаційної безпеки як одного з видів національної безпеки;

✓ розглянути основні типи інформаційних загроз;

✓ окреслити основні модифікації інформаційних потоків (знищення інформації, зашумлення каналів великим обсягом побічної інформації, нав'язування інформації, дезінформування тощо);

✓ визначити роль держави як об'єкта забезпечення інформаційної безпеки;

✓ проаналізувати проблеми України, пов'язані з захистом українського національного інформаційного ринку (процеси глобалізації та інформаційна експансія з боку Росії);

✓ ознайомити студентів із законодавчо-нормативною базою забезпечення захисту інформації.

У процесі вивчення курсу «Інформаційна безпека» студенти повинні оволодіти певною системою **знань, умінь та навичок**, а саме:

✓ знати визначення основних понять курсу (інформаційна політика, інформаційний простір, національні інтереси, національна безпека, інформаційна безпека, інформаційні загрози, захист інформації тощо);

✓ розрізняти види національної безпеки;

✓ уміти аналізувати найтиповіші форми інформаційної експансії в Україну та орієнтуватися в способах протидії інформаційному вторгненню;

✓ знати основні напрями забезпечення інформаційної безпеки та способи застосування цих напрямів на практиці;

✓ знати законодавчі акти в галузі захисту інформації, орієнтуватися в роботі правоохоронних органів та судової системи в галузі захисту інформації.

Методи викладання. Курс викладається один семестр й має обсяг 120 годин. У навчальному процесі застосовуються лекції, семінарські та практичні заняття, самостійна робота студентів, написання рефератів: лекції – 20 годин, практичні – 24 годин, самостійна робота – 72 годин.

2.3. Міждисциплінарні зв'язки

- ✓ історія;
- ✓ політологія;
- ✓ соціологія;
- ✓ правознавство;
- ✓ теорія масової інформації та ін.

2.4. Форми контролю знань і критерії оцінювання з курсу.

Контроль та оцінювання теоретичних знань та практичних навичок студентів протягом навчального семестру відбувається за результатами усних відповідей на практичних заняттях, складанні підсумкового колоквіуму, а також у процесі контролю поточної самостійної роботи.

Робоча програма курсу передбачає застосування таких форм поетапного контролю знань (кожен вид роботи оцінюється за відповідними критеріями в балах):

1) вхідний контроль – написання самостійної роботи (визначення основних категорій, що вивчалися на першому курсі та що необхідні для засвоєння курсу "Інформаційна безпека");

2) поточний контроль – виконання студентами навчальної програми з курсу як в аудиторії, так і позааудиторно:

- ✓ відвідування лекційних занять;
- ✓ робота на семінарах;
- ✓ опрацювання питань самостійної роботи;

✓ виконання індивідуальних завдань (написання реферату або підготовка доповіді);

3) підсумковий (вихідний) контроль:

✓ звіт про виконання індивідуальних завдань;

✓ складання підсумкового колоквіуму;

✓ підрахунок загальної кількості балів (загальна оцінка з дисципліни (100%) включає сукупний результат поточної роботи студента протягом семестру).

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота										Сума
Змістовий модуль №1					Змістовий модуль № 2					
Т 1	Т 2	Т 3	Т 4	Т 5	Т 6	Т 7	Т 8	Т 9	Т 10	100
10	10	10	10	10	10	10	10	10	10	

Шкала оцінювання: національна та ECTS

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
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**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

3. Структура та зміст дисципліни.

3.1. Тематика та зміст практичних (семінарських) занять

Змістовний модуль №1.
Поняття інформаційної безпеки

Тема 1. Основи національної безпеки держави.

1. Основні поняття національної безпеки:

1.1. Визначення національної безпеки.

1.2. Основні категорії теорії національної безпеки.

1.3. Фактори та засоби забезпечення національної безпеки.

2. Характеристика основних видів національної безпеки:

2.1. Рівні національної безпеки.

2.2. Види національної безпеки.

3. Система забезпечення національної безпеки в Україні:

3.1. Визначення системи забезпечення національної безпеки.

3.2. Функції системи забезпечення національної безпеки.

3.3. Повноваження суб'єктів забезпечення національної безпеки.

Рекомендована література

1. Карпенко В. Основи професіональної комунікації / Карпенко В. Київ: Нора- прінт, 2002. 348 с.

2. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Кормич Б. Київ: Кондор, 2004. 384 с.

3. Основи інформаційного права України: навч. посіб. / за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

4. Юдін О. Інформаційна безпека держави: навч. посіб. / О. Юдін, В. Богуш. Х.: Консул, 2005. 576 с.

Тема 2.Основні положення інформаційної безпеки.

1. Поняття інформаційної безпеки:

1.1. Визначення інформаційної безпеки.

1.2. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.

1.3. Об'єкти та суб'єкти інформаційної безпеки.

1.4. Види інформаційної безпеки.

1.5. Концепція інформаційної безпеки держави.

2. Загрози інформаційній безпеці:

2.1. Дестабілізуючі фактори інформаційної безпеки.

2.2. Класифікація загроз інформаційній безпеці.

2.3. Джерела загроз інформаційній безпеці.

3. Методи і засоби забезпечення інформаційної безпеки:

3.1. Основні принципи забезпечення інформаційної безпеки.

3.2. Система забезпечення інформаційної безпеки держави.

3.3. Основні форми і способи забезпечення інформаційної безпеки держави.

Рекомендована література

1. Кормич Б. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

2. Литвиненко О. Інформаційна безпека Європи / Литвиненко В. Київ. 1999.

3. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. Київ: Текст, 2004. 136 с.

4. Основи інформаційного права України: за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

5. Юдін О. Інформаційна безпека держави. Харків: Консул, 2005. 576 с.

<u>Тема 3.</u>Основні поняття інформаційного протиборства.

1. Визначення поняття “інформаційне протиборство”.

2. Інформаційна війна.

3. Інформаційний тероризм.

4. Інформаційна злочинність.

5. Інформаційне протиборство як форма забезпечення інформаційної безпеки.

Рекомендована література.

1. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. Київ: Текст, 2004. 136 с.

2. Потятиник Б. Патогенний текст / Б. Потятиник, М. Лозинський. Львів: Місіонер, 1996. 296 с.

3. Почепцов Г. Информация&дезинформація / Почепцов Г. Київ: Ника- центр, Эльга, 2001. 256 с.

4. Почепцов Г. Как ведуться тайные войны: Психологическиеоперации в современном мире / Почепцов Г. Харків: Консум, 2000. 200 с.

5. Почепцов Г. Теорія комунікації / Почепцов Г. Київ: Видавничо- поліграфічний центр „Київський університет", 1999. 308 с.

6. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

<u>Тема 4.</u>Інформаційна війна як інструмент інформаційного протиборства.

1. Визначення інформаційної війни.
2. Концепція інформаційної війни.
3. Органи інформаційної війни.
4. Основні форми інформаційної війни.

Рекомендована література

1. Карпенко В. Основи професіональної комунікації / Карпенко В. Київ: Нора- прінт, 2002. 348 с.

2. Кормич Б. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

3. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

<u>Тема 5.</u> Інформаційна зброя.

1. Визначення, особливості та сфера застосування інформаційної зброї.

2. Інформаційна зброя воєнного застосування.

3. Інформаційна зброя воєнного та невоєнного застосування.

4. Засоби ураження комп'ютерних інформаційних систем.

5. Засоби ураження (впливу) на людей та їхню психіку.

6. Особливості, що характеризують основні риси застосування інформаційної зброї.

Рекомендована література.

1. Гриценко О. Основи теорії міжнародної журналістики / О. Гриценко, В. Шкляр. Київ: Видавничо-поліграфічний центр „Київський університет", 2002. 304 с.

2. Дубас О. Інформаційний розвиток сучасної України у світовому контексті/ Дубас О. Київ: Генеза, 2004. 208 с.

3. Карпенко В. Антиукраїнські тенденції в українській державі / Карпенко В. Кив: Акціонерне товариство „Київська книжкова фабрика", 2001. 112 с.

4. Кудрявцева С. Міжнародна інформація: / С. Кудрявцева, В. Колос. Київ: Видавничий Дім „Слово", 2005. 400 с.

5. Лизанчук В. Завжди пам'ятай: Ти – Українець! / Лизанчук В. – [2-е вид.]. Львів : Мальва, 2001. 680 с.

6. Основи інформаційного права України: / Цимбалюк В., Павловський В., Грищенко В. та ін.; за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

7. Україна: інформація і свобода слова: збірник законодавчих актів, нормативних документів та статей фахівців / упоряд. А. М. Задворний. Київ: Молодь, 1997. 832 с.

8. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

<u>Тема 6</u>. Основи теорії інформаційної боротьби.

1. Основні визначення теорії інформаційної боротьби.

2. Закони та закономірності інформаційної боротьби.
3. Принципи інформаційної боротьби.
4. Заходи інформаційної боротьби.
5. Способи та форми ведення інформаційної боротьби.
6. Методологія оцінки ефективності інформаційної боротьби.

Рекомендована література

1. Карпенко В. Основи професіональної комунікації / Карпенко В. Київ: Нора- прінт, 2002. 348 с.

2. Кормич Б. Інформаційна безпека: організаційно-правові основи: / Кормич Б. Київ: Кондор, 2004. 384 с.

3. Основи інформаційного права України: за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

4. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. Київ: Текст, 2004. 136 с.

5. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

Тема 7.Психологічна війна та інформаційно-психологічна безпека держави.

1. Поняття психологічної війни. Цілі та завдання психологічної війни.
2. Види та закономірності психологічних впливів.
3. Закономірності психологічного впливу.
4. Основи психологічних операцій.
5. Органи та засоби проведення психологічних операцій.
6. Технології психологічної війни.
7. Основні характеристики об'єктів психологічної війни.
8. Форми та методи впливу в психологічній війні.
9. Особливі способи та прийоми психологічної війни.

Рекомендована література

1. Кормич Б. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

2. Литвиненко О. Інформаційна безпека Європи / Литвиненко В. Київ, 1999.

3. Основи інформаційного права України: за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

4. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

Змістовний модуль №2

Інформаційна безпека в Україні

Тема 8.Інформаційна безпека України.

1. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.

2. Загрози інформаційній безпеці України.

3. Джерела загроз інформаційній безпеці України.

4. Стан інформаційної безпеки України.

5. Завдання і забезпечення інформаційної безпеки України.

Рекомендована література

1. Карпенко В. Основи професіональної комунікації / Карпенко В. – К. : Нора- прінт, 2002. – 348 с.

2. Кормич Б. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

3. Основи інформаційного права України: за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

4. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. Київ: Текст, 2004. 136 с.

5. Юдін О. Інформаційна безпека держави. Харків: Консул, 2005. 576 с.

Тема 9. Методи та заходи забезпечення інформаційної безпеки України.

1. Загальні методи забезпечення інформаційної безпеки України.

2. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя:

2.1. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.

2.2. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.

2.3. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.

2.4. Забезпечення інформаційної безпеки України в галузі науки та техніки.

2.5. Забезпечення інформаційної безпеки України у сфері духовного життя.

2.6. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.

2.7. Забезпечення інформаційної безпеки України у сфері оборони.

2.8. Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.

2.9. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.

3. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.

Рекомендована література

1. Гриценко О. Основи теорії міжнародної журналістики / О. Гриценко, В. Шкляр. Київ: Видавничо-поліграфічний центр „Київський університет”, 2002. 304 с.

2. Дубас О. Інформаційний розвиток сучасної України у світовому контексті. Київ: Генеза, 2004. 208 с.

3. Карпенко В. Антиукраїнські тенденції в українській державі / Карпнко В. Київ: Акціонерне товариство „Київська книжкова фабрика", 2001. 112 с.

4. Кудрявцева С. Міжнародна інформація. Київ: Видавничий Дім „Слово", 2005. 400 с.

6. Основи інформаційного права України: за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

7. Україна: інформація і свобода слова: збірник законодавчих актів, нормативних документів та статей фахівців / упоряд. А. М. Задворний. Київ: Молодь, 1997. 832 с.

8. Юдін О. Інформаційна безпека держави: Харків: Консул, 2005. 576 с.

Тема 10.Система та політика забезпечення інформаційної безпеки України.

1. Основні функції системи забезпечення інформаційної безпеки України.

2. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.

3. Основні положення політики забезпечення інформаційної безпеки України.

4. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

Рекомендована література.

1. Карпенко В. Основи професіональної комунікації / Карпенко В. Київ: Нора- прінт, 2002. 348 с.

2. Кормич Б. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

3. Основи інформаційного права України. за ред. М. Швеця, Р. Калюжного, П. Мельника. Київ: Знання, 2004. 274 с.

4. Харченко Л. Інформаційна безпека України: Глосарій. Київ: Текст, 2004. 136 с.

5. Юдін О. Інформаційна безпека держави. Харків: Консул, 2005. 576 с.

3.2. Методичні рекомендації з підготовки практичних (семінарських) занять.

Мета семінарських занять – поглиблення та закріплення знань, отриманих на лекціях і під час самостійного вивчення окремих тем курсу. Як правило, на семінар виносяться 3–4 питання; їх розглядають як у традиційній формі, так і у вигляді дискусії, розгорнутої бесіди, конференції, "круглого столу", особливо якщо обговорюються проблемні питання. Опитування студентів на семінарі проходить як за бажанням студента, так і за викликом викладача. Крім основних виступів студентів на семінарі, виклададає,оцінює також істотні доповнення до викладеної проблеми. На семінарських заняттях можуть обговорюватися повідомлення, доповіді та реферати.

У кінці заняття викладач підводить підсумки роботи, оцінює виступи і доповнення кожного студента, акцентуючи увагу на найбільш вдалих відповідях, недоліках у висвітленні теми. Крім цього, студенти отримують завдання щодо підготовки до наступного семінарського заняття. Оцінки, одержані на семінарі, обов'язково враховуються при рейтинго-модульній системі контролю знань.

Готуючись до семінарського заняття, студент повинен опрацювати рекомендовані до даної теми джерела та літературу, продумати відповіді на кожне питання, скласти план і стислі тези свого виступу. Важливе значення у підготовці до семінару мають консультації викладачів, час і місце проведення яких доводиться до відома студентів. Готуватися до семінарського заняття необхідно заздалегідь. Всебічна та ґрунтовна підготовка –

важлива передумова створення творчої атмосфери при обговоренні передбачених планом семінару питань, змістовних виступів і доповнень. На семінарі студенти повинні доповнювати свої записи новим матеріалом з виступів своїх товаришів та викладача.

Семінарські заняття базуються на самостійній роботі студентів, яка є однією з основних форм навчального процесу. Лише самостійна робота в комплексі з іншими формами навчання забезпечує глибоке вивчення та всебічне засвоєння студентами матеріалу, оволодіння методами наукового мислення, виховання у них творчих, аналітичних підходів до вивчення дисципліни. Форми самостійної роботи студентів можуть бути різноманітними: вивчення і конспектування документів та інших історичних джерел, навчальної та навчально-методичної літератури, монографій і наукових статей, написання тематичних повідомлень, доповідей, рефератів. Основна ділянка самостійної роботи – уважне читання і конспектування передбачених до семінарського заняття основних джерел та літератури. Це обов'язкова вимога при вивченні інформаційної безпеки, один з головних елементів модульно- рейтингової системи оцінки знань студентів

4. Самостійна робота студентів.

4.1. Мета й завдання самостійної роботи студентів

а) закріплення у студентів умінь і навичок роботи з науковою літературою (конспектування, виписування тез, загальне ознайомлення тощо);

б) закріплення у студентів володіння методикою укладання словника, креслення схем і таблиць;

в) краще усвідомлення та запам'ятовування матеріалу під час виконання завдань для самостійної роботи;

г) систематизування знань під час укладання словника.

4.2. Форми організації самостійної роботи

1. Забезпечити студентів необхідними навчально-методичними матеріалами (підручниками й посібниками, фаховими виданнями, адресами в Інтернеті, текстами лекцій тощо).

2. Чітко визначити зміст і методи виконання завдань для самостійної роботи: – подати чіткий список завдань для самостійного опрацювання відповідно до кожної теми; – до кожного завдання обов'язково вказати джерело й конкретні сторінки, що потрібно опрацювати; – зазначити методи виконання самостійної роботи для кожного конкретного завдання (конспектування, тези, виписки, загальне ознайомлення тощо); – подати чіткий список термінів відповідно до кожної теми із зазначенням джерела, звідки можна виписати дефініцію даних понять.

3. Організувати системний контроль за виконанням студентами завдань для самостійного опрацювання.

3.1. Вхідний контроль: подати питання для повторення положень основних законів, які формують сучасне правове поле інформаційної діяльності.

3.2. Поточний контроль: а) перевіряти виконання студентами індивідуальних завдань; б) перевіряти виконання студентами завдань для самостійного опрацювання; в) перевіряти ведення словника.

3.3. Підсумковий контроль: розробити питання для підсумкового колоквіуму, що проводиться наприкінці вивчення курсу.

4.3. Методичні рекомендації до самостійної роботи.

Курс „Інформаційна безпека" вивчається протягом одного семестру. Навчально-тематичним планом передбачена самостійна робота з найбільш актуальних і складних тем курсу „Інформаційна безпека". На самостійну роботу виносяться основні та додаткові питання і завдання, передбачені запропонованими планами, і вони проводяться під керівництвом викладачів з використанням різних форм та методів

контролю знань студентів: тестування, опитування, вільна дискусія, обговорення реферативних повідомлень, перевірка робочих зошитів, глосарію.

При виконанні самостійної роботи студенти можуть зіткнутися з певними труднощами, пов'язаними, передусім, з браком джерел з дисципліни, що вивчається. У зв'язку з цим студенти мають звернути особливу увагу на: 1) ретельне конспектування лекцій; 2) самостійне вивчення наукових праць, перелік яких дається на лекціях, а також міститься у робочій програмі в розділі „Література". Ураховуючи зазначене, ведення робочого зошиту є доцільним елементом підготовки до занять.

Крім цього, для формування понятійного апарату студентам рекомендовано вести власний тезаурус, в якому відображатимуться ключові терміни, що відповідають конкретній темі. Перелік цих термінів не є жорстко визначеним і залежить від творчого підходу кожного студента, водночас їхній перелік становить базовий мінімум і міститься наприкінці даної програми у розділі „Термінологічний мінімум". За відсутності робочого зошиту із відпрацьованими темами і тезаурусу студенти не зможуть успішно оволодіти даним предметом.

Студенту, під час індивідуальної співбесіди, з обговорення реферату, при висвітленні питань теми дозволяється користуватися робочим зошитом, власним тезаурусом. Студенту можуть ставитися додаткові запитання.

Наприкінці обговорення рефератів, дискусії тощо, викладач оцінює знання студентів і рівень підготовки групи в цілому, наголошує на питаннях, які потребуються більш детального вивчення під час подальшої самостійної роботи.

Завершується вивчення курсу „Інформаційна безпека" складанням іспиту.

4.4. Перелік питань для самостійної роботи

№ з/п	Назва теми	Кількість годин

1	Основи національної безпеки держави.	5/
2	Сутність та зміст інформаційної безпеки у сучасних міжнародних відносинах.	5/
3	Основні положення інформаційної безпеки.	5/
4	Загрози інформаційній безпеці.	5/
5	Методи і засоби забезпечення інформаційної безпеки.	5/
6	Основні поняття інформаційного протиборства.	6/
7	Інформаційна війна як інструмент інформаційного протиборства.	5/
8	Інформаційна зброя.	5/
9	Основи теорії інформаційної боротьби.	5/
10	Психологічна війна та інформаційно-психологічна безпека держави.	5/
11	Інформаційна безпека України.	6/
12	Методи та заходи забезпечення інформаційної безпеки України.	5/
13	Система та політика забезпечення інформаційної безпеки України.	5/
14	Засоби масової інформації та неурядові організації як засіб впливу на інформаційний простір України.	5/
	Разом	72/

4.5.Методичні поради до написання реферату

Реферат (від латин. referre – доповідаю, повідомляю) – це коротке викладення основних положень вчення, наукової чи навчальної проблеми у письмовому чи усному вигляді. Реферат готується, як правило на основі аналізу декількох джерел інформації, зміст яких вільно і компактно викладається у доступній для розуміння формі.

Підготовлений у письмовому вигляді реферат оформляється розбірливим почерком (або друкується), на окремих аркушах паперу формату А-4 із відповідною нумерацією сторінок відповідно з планом, розробленим студентом самостійно. Його обсяг складає не менше 10 – 15 сторінок. Реферат повинен мати характер самостійного дослідження запропонованої літератури.

Вимоги до реферату:

1. Визначити об'єкт і мету спілкування.
2. Добрати відповідну літературу. Щоб реферат був змістовним, необхідно приділити увагу добору матеріалу. А для цього рекомендується використати ряд джерел. Передусім потрібно з'ясувати, яка література існує з теми реферату (за алфавітним, систематичним, тематичним каталогами, бібліографічними виданнями можна знайти необхідну літературу).
3. Працюючи з літературою, потрібно насамперед налаштуватися, дати собі цільову установку: вивчити за книжкою те чи інше питання, яке потрібно висвітлити; критично проаналізувати зміст книжки; перевірити, чи збігається ваша оцінка якоїсь проблеми з думкою автора, інших авторитетних осіб; вибрати для реферату найяскравіші факти, приклади, цікаві положення тощо.
4. Опрацювати джерела з робочими стислими помітками, закладками в книжці.
5. Скласти план відповідно до обсягу реферату (його пункти розкриваються приблизно на однаковій кількості сторінок). План реферату міститься на початку роботи.
6. Текст реферату слід структурувати (виділити розділи, параграфи тощо);
7. Оформити яскравий, оригінальний вступ.
8. Дати аналіз вивченої літератури та запропонувати власну інтерпретацію висновків і фактів, з якими ознайомився студент

під час роботи над основними джерелами. Список використаної літератури розмістити наприкінці реферату.

9. Під час усного виступу краще розповідати, а не читати реферат. Для цього скласти розгорнутий план-конспект на 2-4 сторінки.

10. Під час добору мовних засобів для написання реферату необхідно враховувати особливості наукового стилю мовлення.

4.6. Індивідуальні завдання (теми рефератів)

1. Інформаційна безпека як вид національної безпеки.
2. Загрози інформаційній безпеці.
3. Методи й засоби забезпечення інформаційної безпеки.
4. Країни Європи у світовому інформаційному просторі й системи інформаційної безпеки.
5. Патогенний текст як загроза інформаційно-психологічній безпеці.
6. Основні поняття інформаційної війни: історія і сучасність.
7. Основні поняття та форми психологічної війни.
8. Дезінформування як особливий прийом психологічної війни.
9. Державна політика забезпечення інформаційної безпеки.
10. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
11. Система та політика забезпечення інформаційної безпеки України.
12. Інформаційний простір України як чинник національної безпеки.
13. Інформаційна експансія Росії в український інформаційний простір як загроза національній державності.
14. Засоби масової інформації та неурядові організації як засіб впливу на інформаційний простір України.
15. Поняття та сутність феномену «маніпуляція».
16. Технології маніпулювання свідомістю людини.
17. Механізми масового маніпулятивного впливу.
18. Інформаційна пропаганда: сутність, типи, методи.
19. Країни Європи в світовому інформаційному просторі і системи інформаційної безпеки.

20. Духовно-релігійна складова національної безпеки України.

5. Методичні рекомендації для виконання контрольних робіт.

Навчальний процес в РДГУ передбачає різні форми індивідуальної роботи слухачів, однією з яких є виконання контрольних робіт. Основне завдання контрольної роботи - це формування власної думки слухачів з теоретичних та практичних питань, які розглядаються, та внесення ними пропозицій щодо їх вирішення. Підготовка контрольної роботи повинна розпочатися з вивчення методичних рекомендацій за темою та інших публікацій з питань, що досліджуються. Робота повинна бути виконана слухачами самостійно та належним чином оформлена. Вимоги до оформлення. Контрольна робота виконується і подається слухачем на перевірку викладачеві як в надрукованому вигляді так і допускається її представлення у рукописному варіанті. Сторінки мають бути пронумерованими. Контрольна робота має бути написана українською мовою. Першим листом контрольної роботи є титульний лист. Планом контрольної роботи є завдання за певним варіантом. В контрольній роботі обов'язково перелічуються всі використані джерела наукової літератури та нормативні акти. Література і нормативні акти, що цитуються, повинні бути оформлені у вигляді загального списку у порядку цитування або за абеткою. Цінним додатком до роботи є таблиці та схеми. Таблиці і схеми відокремлюються від основного тексту пустими рядками. Основні висновки, пропозиції та рекомендації необхідно оформляти в заключній частині роботи. Контрольна робота в обов'язковому порядку перевіряється викладачем. Контрольна робота оцінюється за змістом, ступенем самостійності виконання, вмінням під час захисту обґрунтувати основні положення роботи та зроблені в ній висновки.

5.1. Питання на контрольну роботу.

Контрольна робота № 1 Поняття інформаційної безпеки та інформаційної політики

1. Визначення національної безпеки.
2. Основні категорії теорії національної безпеки.
3. Фактори та засоби забезпечення національної безпеки.
4. Рівні національної безпеки.
5. Види національної безпеки.
6. Визначення системи забезпечення національної безпеки.
7. Функції системи забезпечення національної безпеки.
8. Повноваження суб'єктів забезпечення національної безпеки.
9. Визначення інформаційної безпеки.
10. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
11. Об'єкти та суб'єкти інформаційної безпеки.
12. Види інформаційної безпеки.
13. Концепція інформаційної безпеки держави.
14. Дестабілізуючі фактори інформаційної безпеки.
15. Класифікація загроз інформаційній безпеці.
16. Джерела загроз інформаційній безпеці.
17. Основні принципи забезпечення інформаційної безпеки.
18. Система забезпечення інформаційної безпеки держави.
19. Основні форми і способи забезпечення інформаційної безпеки держави.
20. Визначення поняття "інформаційне протиборство".
21. Інформаційна війна.
22. Інформаційний тероризм.
23. Інформаційна злочинність.
24. Інформаційне протиборство як форма забезпечення інформаційної безпеки.
25. Визначення державної інформаційної політики.
26. Поняття про програму входження держави в інформаційне суспільство.
27. Основні напрями національної інформаційної політики у сфері суспільних відносин.
28. Основні напрями національної інформаційної політики в економічній сфері.

29. Основні напрями національної інформаційної політики в організаційній сфері.

30. Основні поняття політики забезпечення інформаційної безпеки держави.

31. Основні загрози інформаційній безпеці держави.

32. Організаційний напрям протидії загрозам у сфері інформаційної безпеки.

33. Захист прав і свобод людини та громадянина.

34. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.

35. Науково-практична робота щодо забезпечення інформаційної безпеки.

36. Удосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.

Контрольна робота № 2 Інформаційна політика та інформаційна безпека в Україні

1. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.

2. Загрози інформаційній безпеці України.

3. Джерела загроз інформаційній безпеці України.

4. Стан інформаційної безпеки України.

5. Завдання і забезпечення інформаційної безпеки України.

6. Загальні методи забезпечення інформаційної безпеки України.

7. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.

8. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.

9. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.

10. Забезпечення інформаційної безпеки України в галузі науки та техніки.

11. Забезпечення інформаційної безпеки України у сфері духовного життя.

12. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.
13. Забезпечення інформаційної безпеки України у сфері оборони.
14. Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.
15. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
16. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.
17. Основні функції системи забезпечення інформаційної безпеки України.
18. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
19. Основні положення політики забезпечення інформаційної безпеки України.
20. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

6. Питання на іспит.

1. Визначеннянаціональноїбезпеки.
2. Основнікатегоріїтеоріїнаціональноїбезпеки.
3. Фактори та засобизабезпеченнянаціональноїбезпеки.
4. Рівні національної безпеки.
5. Види національної безпеки.
6. Визначення системи забезпечення національної безпеки.
7. Функції системи забезпечення національної безпеки.
8. Повноваження суб'єктів забезпечення національної безпеки.
9. Визначення інформаційної безпеки.
10. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
11. Об'єкти та суб'єкти інформаційної безпеки.
12. Види інформаційної безпеки.
13. Концепція інформаційної безпеки держави.
14. Дестабілізуючі фактории інформаційної безпеки.
15. Класифікація загроз інформаційній безпеці.

16. Джерела загроз інформаційній безпеці.
17. Основні принципи забезпечення інформаційної безпеки.
18. Система забезпечення інформаційної безпеки держави.
19. Основні форми і способи забезпечення інформаційної безпеки держави.
20. Визначення поняття “інформаційне протиборство”.
21. Інформаційна війна.
22. Інформаційний тероризм.
23. Інформаційна злочинність.
24. Інформаційне протиборство як форма забезпечення інформаційної безпеки.
25. Визначення державної інформаційної політики.
26. Поняття про программу входження держави в інформаційне суспільство.
27. Основні напрями національної інформаційної політики у сфері суспільних відносин.
28. Основні напрями національної інформаційної політики в економічній сфері.
29. Основні напрями національної інформаційної політики в організаційній сфері.
30. Основні поняття політики забезпечення інформаційної безпеки держави.
31. Основні загрози інформаційній безпеці держави.
32. Організаційний напрям протидії загрозам у сфері інформаційної безпеки.
33. Захист прав і свобод людини та громадянина.
34. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.
35. Науково-практична робота щодо забезпечення інформаційної безпеки.
36. Вдосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.
37. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
38. Загрози інформаційній безпеці України.
39. Джерела загроз інформаційній безпеці України.

40. Стан інформаційної безпеки України.
41. Завдання і забезпечення інформаційної безпеки України.
42. Загальні методи забезпечення інформаційної безпеки України.
43. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
44. Забезпечення інформаційної безпекиУкраїни у сфері внутрішньої політики.
45. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.
46. Забезпечення інформаційної безпеки України в галузі науки та техніки.
47. Забезпечення інформаційної безпекиУкраїни у сфері духовного життя.
48. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.
49. Забезпечення інформаційної безпекиУкраїни у сфері оборони.
50. Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.
51. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
52. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.
53. Основні функції системи забезпечення інформаційної безпеки України.
54. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
55. Основні положення політики забезпечення інформаційної безпеки України.
56. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.
57. Вплив засобів масової інформації та неурядових організацій на інформаційний простір України.
58. Особливості інформаційної війни Росії проти України.

7. Термінологічний мінімум.

Активне забезпечення інформаційної безпеки спрямоване на завчасне виявлення та попередження загроз.

Безпека – стан, при якому кому-небудь, чому-небудь не загрожує небезпека будь-якого виду, існує захист від небезпеки.

Безпека держави – положення, при якому державі не загрожує небезпека. Досягається наявністю ефективного механізму управління і координації діяльності політичних сил та громадських груп, а також активних інститутів (органів) їхнього захисту.

Безпека особистості – положення, при якому особистості не загрожує небезпека. Безпека особистості полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, що дозволили розвивати й реалізовувати соціально значущі здібності й потреби, не зазнаючи при цьому протидії держави й суспільства.

Безпека суспільства – наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи всіх груп населення і протистояти діям, що ведуть до розколу суспільства (зокрема і з боку держави).

Держава – сукупність офіційних органів влади в цій чи іншій країні, основний заклад і спосіб політико-правової організації життя суспільства на чолі з одноособовим або колективним правителем, органами виконавчої та інших видів влади й вертикальною системою управління, за допомогою якої здійснюється влада, охороняється існуючий лад, забезпечується нормальне життя людей.

Державна система забезпечення інформаційної безпеки держави являє собою організаційне об’єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система становить найважливішу ланку системи інформаційної безпеки особистості, суспільства й держави в правовій державі.

Життєво важливі інтереси – сукупність потреб, задовольняння яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства й держави.

Дестабілізуючі фактори – явища та процеси природного й штучного походжень, що породжують інформаційні загрози.

Забезпечення інформаційної безпеки – сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства й держави в інформації.

Загроза – можлива небезпека, тобто здатність заподіяти будь-яку шкоду, призвести до будь-якого нещастя.

Загрози інформаційній безпеці – 1. сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері; 2. дія чи подія, що може призвести до руйнування, спотворення чи несанкціонованого власником чи володільцем доступу до інформаційних ресурсів.

Найбільшу загрозу інформаційній безпеці становить: можливість утрати, порушення цілісності або блокування інформації; відкриття конфіденційної інформації; несанкціоноване використання ресурсів; помилкове використання ресурсів; несанкціонований обмін інформацією; відмова від інформації; відмова від обслуговування.

Інтереси держави в інформаційній сфері полягають у:

✓ створенні умов для гармонічного розвитку інформаційної інфраструктури України;

✓ реалізації конституційних прав і свобод людини й громадянина в галузі одержання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної та соціальної стабільності;

✓ забезпеченні законності та правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва.

Інтереси особистості в інформаційній сфері полягають у:

✓ реалізації конституційних прав особи й громадянина на доступ до інформації, а також на використання інформації в інтересах здійснення діяльності, яка не заборонена законом;

✓ у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у:

✓ забезпеченні інтересів особистості в цій сфері;
✓ зміцненні демократії;
✓ створенні правової соціальної держави;
✓ досягненні й підтримці суспільної злагоди;
✓ у духовному відновленні України.

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційною безпекою варто розуміти єдність захисту наступних компонентів:

✓ системи виробництва інформаційних продуктів;
✓ системи доставки інформаційних продуктів до споживача;
✓ системи виробництва засобів виробництва інформаційних продуктів та їх доставки;
✓ системи виробництва інформаційних технологій;
✓ системи накопичення і збереження інформаційних продуктів;
✓ системи сервісного обслуговування елементів інформаційної інфраструктури;
✓ системи підготовки кадрів.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, уражаючих державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації.

Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо.

Інформаційна безпека України – стан захищеності її національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави.

Інформаційна війна – комплекс заходів і операцій, спрямованих на забезпечення інформаційної переваги щодо потенційного або реального противника.

Інформаційна зброя – сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), що включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі та інформаційні загрози й захист від них доступними законними способами й засобами.

Інформаційна перевага розуміють ситуацію, що надає можливість змінити уявлення противника про дійсну обстановку й позбавити його здатності прогнозувати подальші події та впливати на них.

Інформаційна політика держави – це головні напрями й предмет діяльності держави в галузі інформації.

Інформаційна сфера – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації.

Інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами управління і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційне середовище – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням та споживанням інформації.

Інформаційне суспільство – 1. органічний сегмент глобального інформаційного товариства, а також забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захист національних моральних і культурних цінностей, забезпечення конституційних прав на свободу слова та вільний доступ до інформації; 2. суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми – знань; 3. суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформаційний патронат (захисник) є формою забезпечення інформаційної безпеки фізичних і юридичних осіб із боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори й загрози стану поінформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) та власне захист життєво важливих інтересів цих осіб від інформаційних загроз, або, як ще кажуть, інформаційний захист.

Інформаційні злочини можуть вчинятися із використанням як інформаційно-комп'ютерних, так й інформаційно-психологічних методів впливу.

Концепція слугує юридичним актом, що містить керівні принципи та цільові настанови щодо шляхів, засобів та методів захисту життєво важливих інтересів людини, групи, суспільства та держави.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

Концепція інформаційної війни – система поглядів на інформаційну війну та шляхи її ведення.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Національна безпека – категорія політичної науки (політології), що характеризує стан соціальних інститутів, що забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості, суспільства та держави. Вона відображає зв'язок безпеки з нацією.

Національний інформаційний простір – інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрація, накопичення, збереження, захист і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави.

Національні інтереси держави відображають фундаментальні цінності та прагнення народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення й способи задоволення. Національні інтереси держави та їхня пріоритетність обумовлюються конкретною ситуацією, що складається в країні та за її межами.

Нація – стійка історична спільність людей, що визначається соціальними зв'язками певної формації і характеризується специфічними етнічними рисами, зумовленими особливостями економічного й культурного розвитку, спільністю території, мови, побуту, традицій і звичаїв, а також відображенням цих факторів у суспільній свідомості та суспільній психології.

Особистість – людина як суб'єкт відносин і свідомої діяльності. До життєво важливих інтересів особистості належать, насамперед права і свободи людини й громадянина, зокрема інформаційні.

Пасивне забезпечення інформаційної безпеки передбачає реагування на вже наявні загрози, спрямоване на безпосередню протидію акціям, що є деструктивними щодо соціальної системи.

Поінформованість особистості (суспільства та держави) – задоволення в будь якій мірі потреб в інформації, що призводить

до оволодіння відомостями про навколишній світ та процеси, що відбуваються у ньому.

Система забезпечення національної безпеки – організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства держави.

Суспільство – сукупність форм сумісної діяльності людей, що утворилися в процесі історичного розвитку. Життєво важливі інтереси суспільства зв'язані зі створенням і розвитком вільного, гуманного, високоосвіченого, гармонійного суспільства, заснованого на принципах демократи, бережливого ставлення до своїх традицій і національного надбання, суспільства, що підтримує і всіляко охороняє основний свій осередок – сім'ю.

Теорія національної безпеки – наука, що поєднує у собі прикладні аспекти соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук із метою дослідження суті, змісту, методів, форм і засобів забезпечення безпеки особистості, суспільства та держави.

Тероризм – загроза або використання насильства в політичних цілях окремими особами або групами, що можуть діяти як на боці, так і проти існуючого уряду, коли такі дії, спрямовані на те, щоб уплинути на більше число людей, ніж безпосередні жертви.

7. Список рекомендованої літератури.

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.
2. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. Київ: Видавничо-поліграфічний центр "Київський університет", 2008. 274 с.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ: Видавництво Ліра-К, 2021. 412 с.

4. Інформаційна безпека держави: навч. посіб. для студ. / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
5. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2000. 352 с.
6. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Кормич Б. Київ: Кондор, 2004. 384 с.
7. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. Київ: Державний університет телекомунікацій, 2021. 201 с.
8. Остроухов В.В. Інформаційна безпека (соціально-правові аспекти). Підручник / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. ; за заг. ред. Є.Д.Скулиша. Київ: КНТ. 2010. 776 с.
9. Юдін О. Інформаційна безпека держави: навч. посіб. / О. Юдін, В. Богуш. Харків: Консул, 2005. 576 с.

Додаткова

1. Біла книга протидії дезінформації. Київ: ГО «Інститут інформаційної безпеки» 2022. 62 с.
2. Глобальна та національна безпека: підручник / авт. кол. :В..І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. / за заг. ред. Г.П.Ситника. Київ : НАДУ, 2016. 784 с.
3. Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок; Ін-тпробл. над. безпеки. Київ: Інтертехнологія. 2009. 136с.
4. Дубас О. Інформаційний розвиток сучасної України у світовому контексті / Дубас О. Київ: Генеза. 2004. 208 с.
5. Зелена книга протидії дезінформації / Упоряд. і заг. ред. С. Балан. Київ: ГО «Інститут інформаційної безпеки». 2022. 178 с.
6. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. Київ: КНТ, 2006. 280 с
7. Литвиненко О. Інформаційна безпека Європи / Литвиненко В. Київ, 1999.

8. Мей К. Інформаційне суспільство. Скептичний погляд / Мей К. ; [пер. з англ.]. Київ: К.І.С.. 2004. 220 с.
9. Основи інформаційного права України : навч. посіб. /; за ред. М. Швеця, Р. Калюжного, П. Мельника. К: Знання. 2004. 274 с.
10. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. Київ: Текст, 2004. 136 с.

Інформаційні ресурси

1. Національна бібліотека України імені В. І. Вернадського, електронні фахові видання // www.nbuv.gov.ua
2. Львівська національна наукова бібліотека імені В. Стефаника // http://www.library.lviv.ua/
3. Національна історична бібліотека України :// http://www.dibu.kiev.ua/
4. Національна парламентська бібліотека України //http://www.nplu.org/
5. Офіційне Інтернет-представництво Президента України http://www.president.gov.ua/
6. Офіційний веб-сайт Верховної Ради України http://zakon.rada.gov.ua/
7. Єдиний веб-портал органів виконавчої влади України http://www.kmu.gov.ua/control
8. Офіційний сайт Ради національної безпеки і оборони України http://www.rainbow.gov.ua/
9. Національний інститут стратегічних досліджень http://www.niss.gov.ua/
10. Центр міжнародної безпеки та партнерства https://www.ispc.org.ua/page/3
11. EUvsDisinfo https://euvsdisinfo.eu/