МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Східноєвропейський національний університет імені Лесі Українки
Кафедра національної безпеки

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної і навчальної роботи та рекрутації
проф. Гаврилюк С. В. _____
Протокол № 2 від «16» жовтня 2019 р.

№8416102019

ПРОГРАМА
нормативної навчальної дисципліни

Захист інформації
підготовки бакалавра

галузі знань 12 “Інформаційні технології”
спеціальності 122 “Комп’ютерні науки та інформаційні технології”
освітньо-професійної програми “Комп’ютерні науки та інформаційні технології”

Луцьк – 2019

Програма навчальної дисципліни «ЗАХИСТ ІНФОРМАЦІЇ**»** підготовки бакалавра, галузі знань 12 “Інформаційні технології”, спеціальності 122 “Комп’ютерні науки та інформаційні технології”, за освітньо-професійною програмою “Комп’ютерні науки та інформаційні технології”.

Розробник: Глинчук Л.Я., старший викладач кафедри прикладної математики та інформатики, кандидат фізико-математичних наук

Рецензент: Булатецька Л.В., доцент кафедри прикладної математики та інформатики, кандидат фізико-математичних наук

Програма навчальної дисципліни затверджена на засіданні кафедри прикладної математики та інформатики

протокол № 3 від 02.10.2019 р.

В.о. завідувача кафедри _____ доц. Чепрасова Т. І.

Програма навчальної дисципліни схвалена науково-методичною комісією факультету інформаційних систем, фізики та математики

протокол № 2 від 03.10.2019 р.

Голова науково-методичної
комісії факультету _____ доц. Полетило С.А.

Програма навчальної дисципліни схвалена науково-методичною радою Східноєвропейського національного університету імені Лесі Українки

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">Галузь знань:
12 “Інформаційні технології”
спеціальності 122 “Комп’ютерні науки та інформаційні технології”,
освітньо-професійна програма “Комп’ютерні науки та інформаційні технології”
Освітній ступінь:
бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання – 4</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів
90/3</td><td>Семестр – 8</td></tr>
<tr><td>Лекції 28 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Лабораторні роботи 28 год.</td></tr>
<tr><td>Самостійна робота 26 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
</table>

2. АНОТАЦІЯ КУРСУ:

Дисципліна «ЗАХИСТ ІНФОРМАЦІЇ» належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра. Спрямована на підвищення рівня формування у студентів знань та умінь, які створять теоретичний і практичний фундамент, необхідний для аналізу загроз виникаючих при зберіганні, обробленні та передачі інформації.

Мета навчальної дисципліни: полягає у комплексному викладі теоретичних основ та практичного використання сучасних систем захисту інформації і технологій згідно із загальними підходами в Україні та світі. Розглядаються поняття, класифікація, сфери застосування, складові і ознаки, різні типи підходів, систем і способі захисту інформаційних ресурсів, а також методи використання інформаційних технологій, їх застосування в різних сферах сучасного життя.

Програмні результати навчання:

Бакалавр повинен знати: критерії оцінки інформаційної безпеки; поняття батьківського контролю; найпоширеніші мобільні віруси та засоби боротьби з ними; способи та можливості захисту в соціальних мережах; управління паролями та правила роботи з ними; поняття шкідливого програмного забезпечення; основні

типи та загальний огляд сучасних комп'ютерних вірусів; поняття антивірусної програми та їх класифікацію; основи криптографічного захисту; основи безпеки інформації в комп'ютерних мережах; поняття авторського права та плагіату.

Бакалавр повинен вміти: користуватися засобами резервного копіювання та відновлення даних; пристроями відновлення даних; користуватися можливостями операційної системи для захисту та налаштовувати власний профіль; захищати інформацію на мобільних телефонах; захистити електронну пошту та власні акаунти під час роботи в мережі; користуватися та налаштовувати антивірусні програми; застосовувати програмне забезпечення з використанням криптографії; захищати файли різних форматів; захищати авторські права; виявляти плагіат.

3. КОМПЕТЕНЦІЇ

До кінця навчання студенти будуть компетентними у таких питаннях:

- володіти технологіями та методами розроблення програмного забезпечення для захисту інформації в комп'ютеризованих системах та мережах;
- володіти методами захисту інформації в Інтернет-ресурсах;
- застосовувати алгоритми та методи захисту інформації у проектах комп'ютеризованих систем;
- проводити аналіз дефектів, помилок та ризиків у життєвому циклі програмного забезпечення, обирати та формувати вимоги до характеристик якості;
- контролювати та перевіряти правильність експлуатації встановленого програмного забезпечення комп'ютеризованої системи згідно чинних норм та стандартів;
- контролювати та здійснювати моніторинг працездатності системного та прикладного програмного забезпечення в умовах експлуатації комп'ютеризованих систем.

4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програма навчальної дисципліни складається з таких **змістових модулів**:

1. Захист інформації засобами ОС. Шкідливе ПЗ.
2. Захист інформації: криптографія, антивіруси, плагіат та авторське право.

Структура навчальної дисципліни представляється у вигляді таблиці 2.

Таблиця 2

Назви змістових модулів і тем	Кількість годин						
	Усього	у тому числі					
		Лек.	Практ.	Лаб.	Інд.	Сам. роб.	Конс.
1	2	3	4	5	6	7	8
Змістовий модуль 1. Захист інформації засобами ОС. Шкідливе ПЗ							
Тема 1. Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації	4	2		2			
Тема 2. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних	6	2		2		2	
Тема 3. Захист інформації засобами операційних систем. Налаштування власного профілю. Поняття батьківського контролю	6	2		2		2	
Тема 4. Захист інформації на мобільних телефонах. Огляд найпоширеніших мобільних вірусів та засобів боротьби з ними	8	2		2		2	2
Тема 5. Інформаційна безпека в соціальних мережах. Захист електронної пошти та власних акаунтів під час роботи в мережі	6	2		2		2	
Тема 6. Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями	6	2		2		2	
Тема 7. Поняття шкідливого програмного забезпечення. Основні типи та загальний огляд сучасних комп’ютерних вірусів	8	2		2		2	2
Разом за модулем 1	44	14		14		12	4
Змістовий модуль 2. Захист інформації: криптографія, антивіруси, плагіат та авторське право							
Тема 8. Поняття антивірусної програми. Огляд найпоширеніших антивірусних	6	2		2		2	

програм та їх класифікація							
Тема 9. Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування інформації	6	2		2		2	
Тема 10. Інформаційна безпека держави. Потенційні загрози, засоби їх попередження та ліквідації	6	2		2		2	
Тема 11. Захист файлів різних форматів: doc, pdf, xls та інших	6	2		2		2	
Тема 12. Основи безпеки інформації в комп'ютерних мережах та поняття особистої безпеки користувача персонального комп’ютеру	6	2		2		2	
Тема 13. Поняття авторського права. Захист авторських прав. Поняття комп’ютерного піратства	6	2		2		2	
Тема 14. Поняття плагіату. Загальний огляд програмного забезпечення призначеного для виявлення плагіату	6	2		2		2	
Разом за модулем 2	46	14		14		14	4
Всього годин:	90	28		28		26	8

5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

№ з/п	Тема	Кількість годин
1	Криптографічний захист: симетричні методи шифрування	6
2	Криптографічний захист: асиметричні методи шифрування	6
3	Закон України “Про захист інформації”	4
4	Закон України “Про захист персональних даних”	4
5	Законодавча база з питань захисту інформації країн ЄС	6
Всього		26

6. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

<table>
<tr><td colspan="4">Поточний контроль
(max = 40 балів)</td><td colspan="2">Модульний контроль
(max = 60 балів)</td><td rowspan="3">Загальна кількість балів</td></tr>
<tr><td colspan="4">Модуль 1</td><td colspan="2">Модуль 2</td></tr>
<tr><td colspan="2">Змістовий модуль 1</td><td colspan="2">Змістовий модуль 2</td><td>МКР 1</td><td>МКР 2</td></tr>
<tr><td>Т1</td><td>Т2-Т7</td><td>Т8</td><td>Т9-Т14</td><td rowspan="2">30</td><td rowspan="2">30</td><td rowspan="2">100</td></tr>
<tr><td>2</td><td>3</td><td>2</td><td>3</td></tr>
</table>

Шкала оцінювання (національна та ECTS)

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсової роботи (проекту), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82 – 89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>75 – 81</td><td>C</td></tr>
<tr><td>67 -74</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60 – 66</td><td>E</td></tr>
<tr><td>1 – 59</td><td>Fx</td><td>Незадовільно</td><td>Незараховано (з можливістю повторного складання)</td></tr>
</table>

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». — К.: «МК-Прес», 2005. — 432с., іл.
2. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.

3. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” / укл. С. О. Троян. – Умань : [б.в.], 2012.- 120 с.
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, введений в дію Наказом ДСТСЗІ від 28.04.1999 р. № 22
5. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. — К.: КНТ, 2007.
6. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ України, 2004.
7. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.
8. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
9. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Кормич Б. А.
10. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ України, 2004.
11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.
12. Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.
13. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — К.: НТУУ «КПІ», 2001. — № 4.
14. Петров А.А. Построение комплексной системы защиты информации в сетях общего пользования. / Петров А.А. // Вісник СНУ ім. В.Даля. – 2009. - №136. – С. 135-143.
15. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 336с. 15. Вербицький О.В. Вступ до криптології. — Львів: Видавництво науково-технічної літератури, 1998. — 248 с.
16. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред.
17. С.Г. Лаптєва. — К.: Видавництво Європейського університету, 2001. — 201 с.
18. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МГИФИ, 1997. — 538 с.
19. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. — М.: ТЕИС, 1994. — 69 с.

20. Организация и современные методы защиты информации/Под общ. ред. С.А. Диева, А.Г. Шаваева. — М.: Коцерн “Банковский Деловой Центр”, 1998. — 472 с.
21. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа/Пер. сангл. В. Смирнова. — М.: КРОН-ПРЕСС, 1999. — 816 с.
22. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навч. посібник/За ред. М.Я. Азарова. — Ірпінь: Академія ДПС України, 2003. — 466 с.
23. Хорев А.А. Способы и средства защиты информации. — М.: МО РФ, 2000. — 316 с.
24. Барабаш А.В., Шанкин г.п. История криптографии. Ч.l. — М.: Гелиос АРВ, 2002. — 240 с.
25. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. — М.: НЕЛК, 2001. — 138 с. 27. Попов М.О. До забезпечення воєнної безпеки в умовах загрози інформаційної війни /
26. М.О. Попов, А.Г. Лук'янець // Наука і оборона : наук.-теорет. та наук.-практ. журнал. – 1999. – № 2. – С. 37-43.
27. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В.С. Сідак, В.Ю. Артемов. – К. : Вид-во КНТ, 2007. – 21-24 с.
28. Харченко В.С. Інформаційна безпека : глосарій / В.С. Харченко. – К. : Вид-во КНТ, 2005. – 13-18 с.
29. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України "КПІ", 2001. – № 4. – С. 43-48.
30. http://uk.wikipedia.org/wiki/Інформаційна_безпека_України 33. Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Доступний з http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=2897-17.
31. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.

8. ПЕРЕЛІК ПИТАНЬ ДО ЗАЛІКУ

1. Що називається інформаційною безпекою?
2. Дайте визначення поняття захисту інформації.
3. Назвіть та охарактеризуйте основні властивості інформації.
4. Назвіть та охарактеризуйте основні аспекти захисту інформації та інформаційної безпеки.
5. Які виділяють загрози безпеки інформації відповідно до її властивостей?
6. Назвіть та дайте визначення базовим поняттям інформаційної безпеки.
7. Охарактеризувати шляхи забезпечення інформаційної безпеки держави, підприємства, особистості.
8. Назвати та охарактеризувати основні критерії інформаційної безпеки.
9. Що являють собою законодавчі вимоги до інформаційної безпеки?
10. Що являє собою модель тріади CIA?
11. Що розуміють під резервним копіюванням?
12 Назвіть та охарактеризуйте основні причини пошкодження та руйнування інформації
13. Які ви знаєте вимоги до систем резервного копіювання?
14. Охарактеризуйте кожну з них.
15. Зробіть аналіз видів резервного копіювання.
16. Які ви знаєте способи зберігання резервних копій?
17. Назвіть та охарактеризуйте програми, призначені для резервного копіювання та відновлення даних.
18. Охарактеризуйте основні моменти відновлення даних с жорстких дисків HDD.
19. Опишіть процес резервування вбудованими засобами Windows 7.
20. Як здійснюється процес відновлення даних вбудованими засобами Windows7?
21. Як встановити пароль для облікового захисту?
22. Як здійснюється захист файлів за допомогою шифрування дисків BitLocker?
23. Як здійснюється включення, призупинення роботи та відключення шифрування дисків BitLocker?
24. Що являє собою захист системи?
25. Що ви знаєте про захист доступу до мережі (NAP)?
26. Як реалізується в операційній системі запобігання виконання даних?
27. Опишіть захист, що забезпечується Захисником Windows, в реальному часі.
28. Що являє собою шифрована файлова система (EFS)?
29. Опишіть призначення, можливості, особливості налаштування та використання батьківського контролю, що забезпечується засобами операційної системи.
30. Назвіть та опишіть основні можливості захисту інформації засобами операційної системи.
31. Назвіть причини втрати інформації на мобільних телефонах.
32. Що називається мобільним вірусом?
33. Що є основною метою створення та розповсюдження мобільних вірусів?
34. Назвіть та опишіть відомі вам схеми роботи мобільних вірусів.

35. Які мобільні антивіруси ви знаєте? Опишіть їх основні можливості.
36. Як здійснюється прослуховування мобільного телефону?
37. Назвіть заходи захисту мобільного телефону від прослуховування.
38. Які ви знаєте ознаки прослуховування розмов по мобільному телефоні?
39. Який антивірус може бути встановлений на ваш мобільний телефон? Які його основні властивості?
40. Які вам відомі вірусні програми, що спрямовані на ураження мобільного телефону?
41. Дайте визначення поняття служби соціальних мереж.
42. Назвіть основні властивості служби соціальних мереж.
43. Охарактеризуйте основні методи викрадення аканту користувача соціальної мережі та засоби захисту від них.
44. Що не варто писати в соціальних мережах?
45. Що таке електронна пошта? Назвіть основні способи втрати інформації під час роботи з даним сервісом.
46. Що називається поштовою бомбою?
47. Назвіть та опишіть типові варіанти виходу поштового сервера з ладу.
48. Опишіть способи боротьби із втратою інформації під час роботи з електронною поштою.
49. Сформулюйте правила під час спілкування в соціальній мережі.
50. Сформулюйте основні правила для користувача електронною поштою.
51. Що називається паролем?
52. Яке програмне забезпечення називається менеджером паролів?
53. На які категорії діляться менеджери паролів.
54. Який принцип роботи менеджерів паролів?
55. Що називається онлайн менеджером паролів?
56. Назвіть основні переваги та недоліки онлайн менеджерів паролів.
57. Що являють собою менеджери паролів з бар'єрним захистом?
58. Назвіть правила створення та користування паролями.
59. Назвіть етапи створення надійного паролю.
60. Які програми управління паролями ви знаєте? Опишіть їх основні можливості.
61. Що називається комп'ютерним вірусом?
62. Які існують основні групи вірусів?
63. Опишіть основні типи мережевих черв'яків.
64. Опишіть основні типи троянів.
65. Зробіть аналіз життєвого циклу шкідливих програм.
66. Які існують способи проникнення шкідливої програми на персональний комп'ютер?
67. Назвіть основні ознаки враження вірусом.
68. Поясніть у чому різниця між шифрованим і поліморфним вірусом?
69. Чи достатньо для захисту від зараження шкідливою програмою встановити файлам дозвіл тільки для читання? Обґрунтуйте відповідь.
70. Поясніть у чому відмінність понять вірус і шкідлива програма.
71. Що називається антивірусною програмою?
72. Назвіть дві основні групи методів антивірусного захисту.
73. Опишіть принципи роботи, переваги та недоліки сигнатурного та евристичного методів антивірусного захисту.

74. З яких основних модулів складається сучасне антивірусне програмне забезпечення?
75. Що таке карантин?
76. Які ви знаєте сучасні найпоширеніші антивірусні програми?
77. Охарактеризуйте можливості більшості сучасних антивірусних програм.
78. Який антивірус встановлений на вашому робочому комп'ютері? Охарактеризуйте його основні можливості.
79. Дайте визначення поняттям «криптографія», «криптографічні методи захисту інформації», «шифрування».
71 Назвіть основні групи шифрування.
72. Що таке кодування? Які типи кодування ви знаєте?
73. В чому суть методів розтину та стиснення даних?
74. Що розуміють під стійкістю шрифту?
75. Сформулюйте основні вимоги до методів криптографічного перетворення.
76. Яка головна мета шифрування (кодування) інформації?
77. Охарактеризуйте способи реалізації криптографічного захисту.
78. Що таке криптографічні алгоритми? На які групи вони поділяються, охарактеризуйте їх.
79. Сформулюйте вимоги до криптографічних методів.
80. Охарактеризуйте програмний комплекс криптографічного захисту інформації «Криптосервер».
81. Що розуміють під інформаційною безпекою держави?
82. Назвіть найбільш небезпечні джерела загроз інтересам держави в інформаційному суспільстві.
83. Назвіть та охарактеризуйте рівні забезпечення інформаційної безпеки.
84. Охарактеризуйте основні національні інтереси України в інформаційній сфері.
85. Назвіть принципи забезпечення інформаційної безпеки України.
86. Що ви розумієте під поняттям «інформаційна війна»?
87. Назвіть складові інформаційної війни.
88. Охарактеризуйте основні елементи інформаційної боротьби.
89. Які ви знаєте види джерел загроз інформаційній безпеці України?
90. Чим визначається поняття "загроза інформаційній безпеці"?
91. Як захистити файли з розширенням doc?
92. Як оцінити захист файлу з розширенням doc?
93. Як захистити файли з розширенням pdf?
94. Як оцінити захист файлу з розширенням pdf?
95. Як захистити файли з розширенням xls?
96. Як оцінити захист файлу з розширенням xls?
97. Які способи захисту файлів ви знаєте?
98. Дайте визначення поняттю «мережева атака».
99. Назвіть основні небезпеки втрати інформації під час роботи в мережі.
100. Охарактеризуйте основні сервіси безпеки.
101. Зробіть аналіз специфічних механізмів безпеки.
102. Опишіть механізм захисту мережі за допомогою міжсіткового екрану.
103. Як уникнути втрату інформації під час роботи з командними файлами в мережі?

104. Як здійснюється захист веб-серверів?
105. Дайте аналіз процесу аутентифікації у відкритих мережах.
106. Як здійснюється захист потоків корпоративних даних, що передаються по відкритих мережах?
107. Проаналізуйте особливості захисту інформації в мережах WiFi.
108. Що називається центром безпеки Windows?
109. Які головні компоненти системи безпеки комп'ютера контролює центр безпеки?
110. Як здійснюється сповіщення про стан системи безпеки на комп'ютері?
111. Опишіть процес налаштування автоматичного оновлення Windows.
112. Які основні небезпеки втрати інформації під час роботи з персональним комп'ютером?
113. Опишіть основні заходи безпеки під час роботи з персональним комп'ютером.
114. Сформулюйте основні поради безпечної роботи з електронною поштою та Інтернетом.
115. Як забезпечити захист USB носія?
116. Що охоплює поняття інтелектуальної власності?
117. Що являє собою авторське право?
118. Що називається піратством? А комп'ютерним піратством?
119. Охарактеризуйте найбільш типові форми комп'ютерного піратства.
120. Дайте аналіз основним формам захисту авторських прав.
121. Охарактеризуйте типові ситуації, що призводять до порушення авторських прав на комп'ютерні програми.
122. Назвіть рекомендації щодо попередження порушень авторських прав на комп'ютерні програми.
123. Охарактеризуйте не юридичні ризики використання неліцензійного ПЗ.
124. Перерахуйте ключові недоліки неліцензійного ПЗ порівняно з ліцензійним.
125. Що охоплює поняття плагіату? Назвіть різні варіанту тлумачення даного терміну.
126. Назвіть та охарактеризуйте найпоширеніші програми для виявлення плагіату.
127. Зробіть аналіз програми, призначеної для виявлення плагіату "Антиплагіат".
128. Які процедури використовують у своїй роботі програми для виявлення плагіату?
129. Назвіть основні правила цитування.
130. Охарактеризуйте програми для виявлення плагіату в програмному коді які ви знаєте.
131. Яку шкоду несе в собі явище плагіату?
132. Як законодавством України карається плагіат?