МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет (інститут) _ інформаційних технологій і математики_____
Кафедра _Комп'ютерних наук та кібербезпеки_

СИЛАБУС

нормативної навчальної дисципліни

_____Вступ до фаху_____

(назва дисципліни)

підготовки _____першого (бакалаврського) рівня_____

(назва освітнього рівня)

спеціальності __125 Кібербезпека_

(шифр і назва спеціальності)

освітньої програми

«Інформаційна безпека»

(назва освітньо-професійної освітньо-наукової/освітньо-творчої програм)

Луцьк – 2020

Силабус навчальної дисципліни «Вступ до фаху» підготовки першого (бакалаврського) рівня вищої освіти, галузі знань 12 Інформаційні технології, спеціальності 125 «Кібербезпека», за освітньою програмою «Інформаційна безпека»

Розробник: Сачук Ю.В., ст. викл., к. фіз.-мат.н.

Силабус навчальної дисципліни затверджено на засіданні кафедри Комп'ютерних наук та кібербезпеки
протокол № _3__ від 5 _жовтня_ 2020 р.

Завідувач кафедри:  (__Сачук Ю.В.__)

І. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня /освітньо-наукова/освітньо-творча програма, освітній рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="5">Галузь знань: 12 Інформаційні технології

Спеціальність: 125 «Кібербезпека»

Освітня програма: «Інформаційна безпека»

Освітній рівень: бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання_2020-2021____</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів 135/4,5</td><td>Семестр__1__-ий__</td></tr>
<tr><td>Лекції _32_ год.</td></tr>
<tr><td>Практичні (семінарські) - год.
Лабораторні _32_ год.
Індивідуальні - год.</td></tr>
<tr><td>Самостійна робота _63_ год.</td></tr>
<tr><td>ІНДЗ: немає</td><td>Консультації 8 год.
Форма контролю: екзамен</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></td></tr>
</table>

ІІ. Інформація про викладача (- ів)

ПІП _Сачук Юрій Володимирович_____

Науковий ступінь _кандидат фізико-математичних наук_____

Вчене звання _____-_____

Посада _старший викладач_____

Контактна інформація +380666587065, e-mail: sachykyra@gmail.com

Дні занять http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис дисципліни

1. Анотація курсу

Предметом навчальної дисципліни «Вступ до фаху» є теоретичні знання забезпечення захисту інформації, засвоєння нормативно-правової галузі в різних сферах захисту інформації. Дисципліна передбачає набуття знань та умінь із організації захисту інформації на об’єктах інформаційної діяльності в цивільній та військових галузях.

Вивчення змісту дисципліни передбачає досягнення такого кваліфікаційного рівня підготовки бакалаврів, за якого студент повинен:

а) знати:

- знатимуть нормативно-методичну базу в галузі кібербезпеки;

- етапи організації та забезпечення безпеки інформації;
- підходи у визначені об’єктів захисту;
- національну та міжнародну нормативно правову базу, науково-методичні та технічні принципи організації впровадження та застосування заходів захисту державних інформаційних ресурсів, інформації з обмеженим доступом в ІС, ТС;
- моделі порушників та типові загрози безпеці інформаційним ресурсам ІС, ТС, ІТС державних органів, установ, організацій та підприємств ;
- проблеми, стан та перспективи створення та застосування заходів захисту державних інформаційних ресурсів, інформації з обмеженим доступом в ІС, ТС, ІТС;
-
-

б)уміти:

- оцінювати збитки внаслідок реалізації загроз інформаційним ресурсам;
- організаційну створювати модель системи об'єктів захисту;
- складати окремі моделі загроз та порушників;
- оцінювати ризики для інформаційних ресурсів;
- розробляти політику безпеки організації;
- складати моделі загроз безпеці інформації, визначати задачі захисту інформації;

2. Мета і завдання навчальної дисципліни

Мета: засвоєння студентами сукупності загроз інформаційної безпеки; загроз кібербезпеки і безпеки інформаційним ресурсам держави; отримання студентами необхідних знань з правових основ захисту інформації в Україні, компетенцій державних установ та інститутів щодо захисту інформації; формування компетенції втілення в життя положень державної політики в сфері захисту інформаційних ресурсів відомств, установ, організацій та підприємств.

Завдання: вивчення основних моделей порушників у сфері кібернетичної безпеки, сучасної методології кібербезпеки як науки, провідних теоретичних концепцій, понятійно-категоріального апарату науки. Аналіз напрямків розвитку інформаційної та кібербезпеки, головні публікації з цієї тематики; вимоги до професійних якостей фахівця з кібербезпеки; класифікацію інформаційних та кібер загроз, освоєння послідовності і методики наукового пошуку, правила написання і оформлення студентського наукового дослідження. Застосовування методик аналітичного аналізу емпіричних даних; здійснення самостійного пошуку джерел і наукової літератури; класифікація інформаційних джерел та здійснення критичного

аналізу джерел; узагальнення стохастичних даних, опрацювання нормативних документів та стандартів у сфері кібербезпеки.

3. Результати навчання (Компетентності)

Інтегральна компетентність. Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у галузі інформаційної, бібліотечної та архівної справи або у процесі навчання, що передбачає застосування положень і методів інформаційної, бібліотечної та архівної справи і характеризуються комплексністю та невизначеністю умов.

Загальні компетентності.

1. Здатність застосовувати знання у практичних ситуаціях. (ЗК 1).
2. Знання та розуміння предметної області та розуміння професії. (ЗК 2).
3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.. (ЗК4).
4. Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5).
5. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. (ЗК 7).

Спеціальні (фахові, предметні) компетентності.

1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. (ФК 1).
2. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. (ФК 8).

Програмні результати навчання

1. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. (ПРН 2)
2. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. (ПРН 4)
3. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. (ПРН 5)
4. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. (ПРН 7)

5. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. (ПРН 8)

1. Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лаб.	Сам. роб.	Конс.	Форма контролю / Бали
Змістовий модуль 1. ЗАГАЛЬНІ ПРИНЦИПИ БЕЗПЕКИ у СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ						
Тема 1. Академічна доброчесність та відповідальність у закладах вищої освіти	6	2		4		РК+ДС / 5
Тема 2. Предмет та завдання дисципліни її місце у системі підготовки фахівців	13	4	4	4	1	РК+ДС / 5
Тема 3. Інформаційна та кібернетична безпека: основні складові, спільні та відмінні ознаки	19	4	4	10	1	РК+ДС / 5
Тема 4. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози	18	4	4	9	1	РК+ДС / 5
Тема 5. Заходи із захисту інформації (мереж і систем) від кіберзагроз та їхній зміст	18	4	4	9	1	РК+ДС / 5
Тема 6. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу	18	4	4	9	1	РК+ДС / 5
Тема 7. Нові загрози з кібербезпеки на основі звітів корпорації Cisco	23	6	6	9	2	РК+ДС / 5
Тема 8. Перспективи та досягнення у сфері кібербезпеки в провідних державах.	20	4	6	9	1	РК+ДС / 5
Разом за модулем 1	135	32	32	63	8	40
Види підсумкових робіт						Бал
Модульна контрольна робота 1						30
Модульна контрольна робота 2						30

Всього годин	135	32	32	63	8	100

2. Питання для самостійного опрацювання

№ з/п	Тема	Години
1.	Основні положення щодо організації системи захисту інформації	8
2.	Визначення інформаційних ресурсів, що підлягають захисту	10
3.	Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту	9
4.	Основи захисту від руйнівних програмних впливів.	9
5.	Рівні захисту інформаційних систем. Основні принципи захисту інформації.	9
6.	Політика інформаційної безпеки на об’єктах критичної інфраструктури	9
7.	Структура забезпечення інформаційної безпеки (Information Security Governance)	9

IV. Політика оцінювання

Політика викладача щодо студента. Відвідування занять є обов’язковим компонентом оцінювання, за яке нараховуються бали. За об’єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі (змішана форма навчання) за погодженням із керівником курсу.

Політика щодо академічної доброчесності. Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 30%. Списування під час контрольних робіт та екзаменів заборонені (в т. ч. із використанням мобільних пристроїв).

Політика щодо дедлайнів та перескладання. Відвідування занять є обов’язковим компонентом оцінювання, за яке нараховуються бали. За об’єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі (змішана форма навчання) за погодженням із керівником курсу.

V. Підсумковий контроль

На іспит виносяться основні питання, типові та комплексні задачі, ситуації, завдання, що потребують творчої відповіді та уміння синтезувати отриманні знання і застосовувати їх під час розв'язання практичних задач.

Остаточна оцінка за курс розраховується наступним чином:

Види оцінювання	% від остаточної оцінки
Опитування під час занять (захисти лабораторних робіт)	40
Модуль 1 (теми 1-8) – модульна контрольна робота	60
Екзамен (теми 1-8) –завдання	60

Основні запитання, що виносяться на екзамен:

1. Що розуміється під терміном "інформація", і які її, істотні з поглядузахисту, властивості?
2. Які є види інформації за режимом доступу?
3. Якими чинниками обумовлюється розвиток захисту інформації в Україні?
4. Які є основні загрози безпеці інформації в Україні?
5. Визначити об`єкти інформаційної небезпеки.
6. Окреслити суб`єктів забезпечення інформаційної безпеки.
7. Визначити джерела та об'єкти інформаційної небезпеки та їх обґрунтування.
8. Обґрунтувати твердження, що кібернетика є об`єктом небезпеки.
9. Розкрити сутність та надати визначення поняття «кібернетична безпека» (кібербезпека).
10. Окреслити та обґрунтувати тотожності та відмінності понять "інформаційна безпека" та «кібернетична безпека» (кібербезпека)
11. Якими основними ознаками характеризується кіберпростір?
12. Окреслити основні положення Доктрини інформаційної безпеки України.
13. Визначити плюси та мінуси соціальних мереж.
14. Розкрити сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя».
15. Здійснення, за вказівкою викладача, пошуку законодавчих активу сфері забезпечення інформаційної безпеки по визначеним критеріям, завданням, висловленням.
16. Моделювання, за вказівкою викладача, тестових завдань з різних дисциплін, які потребують оцінки можливих наслідків с точки зору забезпечення інформаційної безпеки.
17. Назвіть основі заходи в Україні для забезпечення кіберьезпеки.
18. Назвіть основні напрямки діяльності кіберзлочинності?
19. Опишіть взаємозв'язок інформаційного на кіберпросторів.

20. Опишіть дійові особи кіберпростору та їхній вплив на інформаційну і кібербезпеку.
21. Назвіть та опишіть об’єкти впливу в інформаційному та кіберпросторі.
22. Опишіть структуру поняття «інформаційна безпека».
23. Ххарактеризуйте інформаційні системи та технології як об’єкти ІБ.
24. Які є Способи нанесення збитку інформаційній безпеці?
25. Назвіть та опишіть основні методи забезпечення інформаційної безпеки.
26. Назвіть та опишіть складові кібернетичної безпеки.
27. Опишіть критично важливі складові фізичної, інформаційної та кіберінфраструктури.
28. Охарактеризуйте сутність кібернетичної безпеки.
29. Охарактеризуйте інциденти у сфері високих технологій: характерні ознакита проблемні аспекти.
30. Опишіть процедуруобрання раціонального варіантареагування на кібернетичні втручання і загрози.
31. Зобразіть та охарактеризуйте діаграму виникнення інцидентів у сфері високих технологій.
32. Якими основними ознаками характеризується кіберпростір?
33. Класифікація джерел інцидентів, а також способів, об’єктів та результатівїхнього впливу.
34. Схематично зобразіть та охарактеризуйте процес управління інцидентами ІБ.
35. Що належить до найбільш небезпечних інцидентів у сфері кібербезпеки?
36. Опишіть перелік небезпечних векторів атак?
37. Кібератаки та кібертероризм: поняття і визначення.
38. Особливостіреалізації атак і заходи з послаблення їхнього деструктивного впливу
39. Опишіть загальну структура кібернетичної атаки.
40. Опишіть алгоритм реалізації кібератаки.
41. Опишіть фактори, що впливають на інформаційну безпеку.
42. Схематитично зобразіть та опишіть індустрію сучасного кібертероризму.
43. Назвіть основні риси кібертероризму. Що сприяє сучасним терористам у веденні їх протиправної діяльності та забезпечує їм успіх?
44. Назвіть головні прийоми, якими користуються сучасні кібертерористи у процесі своєї протиправної діяльності.
45. Які чинники впливають на поширення кібертероризму в Україні?
46. Назвіть основні типи кібератак за класифікацією П. Ноймана.
47. Назвіть найбільш критичні заходи захисту інформації від кіберзагроз.
48. На основі звіту Циско опишіть тактику ухилення від «пісочниці».
49. На основі звіту Циско розкажіть про розвиток шкідливих програм.
50. На основі звіту Циско розкажіть про загрози з боку електронної пошти.

51. На основі звіту Циско коротко розкажіть про поняття Інтернет речей та DDoS-атаки.
52. На основі звіту Циско коротко розкажіть уразливості та використання патчів.

VI. Шкала оцінювання

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	82-89	добре
C	75-81	добре
D	67-74	задовільно
E	60-66	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом

VI. Рекомендована література та інтернет-ресурси

Основна:

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2008. – 223 с.

2. Лужецький В. А. Інформаційна безпека : навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с. – ISBN 978-966-641-265-5

3. Лужецький В. А. Захист персональних даних : навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с. – ISBN 978-966-641-317-1

4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.

5. Закон України «ПРО захист інформації в інформаційно-телекомунікаційних системах» - відомості Верховної Ради України ШВР),1994.N31.CT.286

6. Закон України "Про основні засади забезпечення кібербезпеки України11- відомості Верховної Ради ПЗВР). 2017. № 45. ст.403;

7. «Доктрина інформаційної безпеки України», затверджено УказомПрезидента України від 25 лютого 2017 року № 47/2017.

8. Постанова Кабінету Міністрів «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. № 266

9. Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. № 96.

10. Постанова Кабінету Міністрів «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12,2015 №1187Наказ МОН України №166 «Деякі питання оприлюднення інформації про діяльністьвищих навчальних закладів» від 19.02.2015 р.

11. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. № 1229;

12. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 р. № 505;

13. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

14. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формуваннятаперевіряння».

15. ДСТУ ITU-TRec.X.509 | ISO/IEC 9594-8:2006 «Інформаційнітехнології. Взаємозв'язок відкритих систем.Каталог:Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів».

16. ДСТУ ISO/IEC 10118-1:2003. Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення

17. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3: Спеціалізовані геш - функції».

18. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування».

19. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».

20. ДСТУ ISO/IEC 13888-1-2002. Інформаційні технології. Методи захисту. Неспростовність. Частина 1. Загальні положення

21. ДСТУ ISO/IECTR 13335-1:2003 «Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки ІТ», 2005

22. ДСТУ ISO/IEC 15946-4. «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 4: Цифровіпідписизвідновленнямповідомлень».

23. ДСТУ ISO/IEC 15946-3:2006 Інформаційні технології. Методи захисту. Криптографічні методи, що грунтуються на еліптичних кривих. Частина 3. Установлення ключів.

Додаткова:

1. Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices [Електронний ресурс] / Damien Stehlé, Ron Steinfeld // Cryptology ePrint Archive. – 2013. – (Report 2013/004). – Режим доступу: http://eprint.iacr.org/2013/004.

2. Обзор методов вичисления дискретного логарифма [Електронний ресурс]. – Режим доступу: Http://WWW. cs. Toronto. edu/~cvs/dlog/research_paper. pdf

3. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс]. – Режим доступу: http://dstszi. gov. ua/dstszi/control/uk/publish/

4. Технологии аутентификации [Електронний ресурс]. – 2009. – Режим доступу: http://ypn. ru/category/data-protection-technologies/authentication-technologies/

5. Факторизація RSA-768 [Електронний ресурс]. – Режим доступу: Https://eprint. jacr. org/2010/006

6. A hybrid lattice-reduction and. meet-in-the-middle attack against NTRU. Nick

38. National Institute of Standards and Technology, FIPS 140-3 (DRAFT), Security for cryptographis modules [Електронний ресурс]. – Режим доступу: http://www. nist. gov/cmvp

39. NESSIE security report: Public Report / B. Preneel, A. Biryukov, E. Oswald and others. – Deliverable D 20 [Електронний ресурс]. – Version 1, 2002. – Режим доступу: http://cryptonessie. org

40. N. Howgrave-Graham, J. H. Silverman, A. Singer, W. Whyte, Modified Parameter Attacks:

41. Practical Attacks Against CCA2 Secure Cryptosystems, and Countermeasures. Preprint available [Електронний ресурс]. – Режим доступу: from http://eprint. iacr. org

42. N. Howgrave-Graham, J. H. Silverman, W. Whyte, A meet-in-the-middle attack on an NTRU private key, NTRU Technical Report 004 [Електронний ресурс]. – Version 2, 2003. – Режим доступу: http://www. ntru. com/cryptolab/tech_notes. htm#004.

43. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. – April, 2000. – Режим доступу: http://csrc. nist. gov/publications/nistpubs//SP800-22rev1a. pdf

44. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for. [Електронний ресурс]. – Режим доступу: http://www. itl. nist. gov/div893/staff/soto/jshome. html

45. NTRU Cryptosystems. Technical reports. [Електронний ресурс]. – Режим доступу: http://www. ntru. com, 2003

46. NTRUEncrypt криптосистема будущего? [Електронний ресурс]. – Режим доступу: http://habrahabr. ru/blogs/crypto/127878/