**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.**

№7916102019

**ПРОГРАМА**
**нормативної навчальної дисципліни**

# Технічний захист інформації

**підготовки бакалавра**

**галузі знань: 12 Інформаційні технології**
**спеціальності 125 Кібербезпека**
**освітньо-професійної програми (спеціалізації) Інформаційна безпека**

Луцьк – 2019

**Програма навчальної дисципліни** “ТЕХНІЧНИЙ ЗАХИСТ ІФНОРМАЦІЇ” підготовки бакалавра, галузі знань 12 “Інформаційні технології”, спеціальності 125 “Кібербезпека”, за освітньо-професійною програмою (спеціалізацією) “Інформаційна безпека”.

**Розробник:** Глинчук Л. Я., кандидат фізико-математичних наук, старший викладач кафедри національної безпеки.

**Рецензент**: Кузьмич О. І., кандидат фізико-математичних наук, доцент кафедри комп’ютерної інженерії та кібербезпеки ЛНТУ

**Рецензент**: Булатецька Л. В., кандидат фізико-математичних наук, доцент кафедри прикладної математики та інформатики СНУ ім. Лесі Українки

**Програма навчальної дисципліни затверджена на засіданні кафедри національної безпеки**

протокол № ___ від _____ 2019 р.

Завідувач кафедри: _____(М. А. Наход)

**Програма навчальної дисципліни схвалена науково-методичною комісією факультету історії, політології та національної безпеки**

протокол № ____від _____ 2019 р.

Голова науково-методичної
комісії факультету _____(А. Г. Шваб)

**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” спеціальність 125 “Кібербезпека” освітньо-професійна програма (спеціалізація) “Інформаційна безпека” Освітній ступінь: бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання – 3</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 150/5</td><td>Семестр – 6</td></tr>
<tr><td>Лекції 34 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Практичні (семінарські) 18 год.</td></tr>
<tr><td>Самостійна робота 88 год.</td></tr>
<tr><td>Консультації 10 год.</td></tr>
<tr><td>Форма контролю: екзамен</td></tr>
</table>

## 2. АНОТАЦІЯ КУРСУ:

Дисципліна “ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ” належить до переліку нормативних навчальних дисциплін програми підготовки бакалавра. Спрямована на підвищення рівня обізнаності щодо нормативно-правової бази у сфері ТЗІ та технічних засобів захисту інформації. У курсі викладені основні положення та нормативні акти для ТЗІ, канали витоку інформації, фізичні та апаратні засоби захисту інформації.

**Мета навчальної дисципліни**: полягає в освоєння принципів побудови ТЗІ в комп’ютерних системах, а також формування умінь використовувати на практиці набуті знання для аналізу захищеності сучасного обладнання та програмного забезпечення, проектування та експлуатації ефективної системи захисту інформації від несанкціонованого доступу. Формування професійних навиків у студентів.

**Програмні результати навчання:**

*Бакалавр повинен знати:* суть нормативно-правових актів України та вимог ДСТСЗІ СБ України щодо організації ТЗІ в комп’ютерних системах; порядок створення комплексів ТЗІ; роль та місце ТЗІ в комп’ютерних системах в комплексній системі захисту інформації (КСЗІ) на об’єкті інформаційної діяльності; орієнтуватися в сучасних системах захисту інформації, методах

проектування та аналізу принципів дії обладнання ТЗІ; класифікацію каналів витоку інформації, фізичні та апаратні засоби захисті інформації.

*Бакалавр повинен вміти:* реалізувати облік, обробку, зберігання, передачу, організацію використання різних носіїв конфіденційної інформації; виявляти й блокувати канали і методи несанкціонованого доступу до інформації, джерела і способів дестабілізуючого впливу на інформацію; встановлювати та адаптувати системи і засоби забезпечення захисту інформації; здійснювати контроль якості функціонування устаткування захищених інформаційних систем, аналізувати якісні і кількісні показники функціонування устаткування, діагностувати й усувати відмови, настроювати та ремонтувати устаткування; самостійно розробляти і вести технічну документацію.

## 3. КОМПЕТЕНЦІЇ

**Загальні компетенції:**

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

**Фахові компетенції:**

КФ 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.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ 11. Здатність виконувати моніторинг процесів функціонування

інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

## 4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

1. Нормативно-правова база у сфері ТЗІ та порядок створення комплексів ТЗІ.

2. Технічні засоби забезпечення захисту інформації.

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. Нормативно-правова база у сфері ТЗІ та порядок створення комплексів ТЗІ** | | | | | | | |
| Тема 1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням. Положення про державну експертизу в сфері технічного захисту інформації | 16 | 4 | 2 | | | 10 | |
| Тема 2. Порядок створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності | 16 | 4 | 2 | | | 10 | |
| Тема 3. Порядок проведення перед проектних досліджень на об’єкті інформаційної діяльності | 16 | 4 | 2 | | | 10 | |
| Тема 4. Рекомендації щодо | 14 | 2 | 2 | | | 8 | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності | | | | | | | |
| Тема 5. Система технічного захисту інформації в Україні: стан та напрями розвитку | 6 | 2 | | | | 2 | 2 |
| Разом за модулем 1 | 68 | 16 | 8 | | | 40 | 4 |
| **Змістовий модуль 2. Технічні засоби забезпечення захисту інформації** | | | | | | | |
| Тема 6. Перехоплення даних. Класифікація каналів витоку інформації. Технічні канали витоку інформації | 16 | 4 | 2 | | | 10 | |
| Тема 7. Методи за засоби захисту від витоку інформації | 8 | 2 | | | | 2 | 4 |
| Тема 8. Поняття інженерно-технічного захисту. Фізичні засоби захисту: охоронні системи, охоронне телебачення, охоронне освітлення та засоби охоронної сигналізації | 14 | 4 | 2 | | | 8 | |
| Тема 9. Апаратні засоби захисту. Ключові елементи: ключові дискети, USB- та LPT-ключі, персональні кодові карти, персональний ідентифікатор, пристрої розпізнавання голосу користувача чи форми його пальців | 16 | 4 | 2 | | | 10 | |
| Тема 10. Класифікація закладних пристроїв, їх основні характеристики та застосування. Способи та засоби боротьби. | 14 | 2 | 2 | | | 10 | |
| Тема 11. ТЗІ на мережевому рівні | 14 | 2 | 2 | | | 8 | 2 |
| Разом за модулем 2 | 82 | 18 | 10 | | | 48 | 6 |
| **Всього годин:** | 150 | 34 | 18 | | | 88 | 10 |

## 5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

| № з/п | Тема | Кількість годин |
|---|---|---|
| 1 | Класи безпеки інформаційних систем | 10 |
| 2 | Загрози безпеці інформації. Основні поняття та класифікація загроз | 12 |
| 3 | Порушники інформаційної безпеки, їх класифікація. Модель поводження потенційного порушника | 10 |
| 4 | Технічна специфікація X.800 | 12 |
| 5 | Критерії оцінювання безпеки інформаційних технологій | 10 |
| 6 | Моделі управління доступом | 12 |
| 7 | Апаратні засоби захисту в мережах | 12 |
| 8 | Апаратні засоби захисту інформації на ринку України | 10 |
| **Разом** | | 88 |

## 6. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

| **Поточний контроль (max = 40 балів)** | | | | | | | | | | | **Модульний контроль (max = 60 балів)** | | **Загальна кількість балів** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Модуль 1** | | | | | | | | | | | **Модуль 2** | | |
| **Змістовий модуль 1** | | | | | **Змістовий модуль 2** | | | | | | **МКР 1** | **МКР 2** | |
| Т1 | Т2 | Т3 | Т4 | Т5 | Т6 | Т7 | Т8 | Т9 | Т10 | Т11 | 30 | 30 | 100 |
| 3 | 3 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | | | |

**Шкала оцінювання (національна та ECTS)**

| **Сума балів за всі види навчальної діяльності** | **Оцінка ECTS** | **Оцінка за національною шкалою** | |
|---|---|---|---|
| | | **для екзамену, курсової роботи (проекту), практики** | **для заліку** |

| | | | |
|---|---|---|---|
| 90 – 100 | A | Відмінно | Зараховано |
| 82 – 89 | B | Добре | |
| 75 – 81 | C | | |
| 67 -74 | D | Задовільно | |
| 60 – 66 | E | | |
| 1 – 59 | Fx | Незадовільно | Незараховано (з можливістю повторного складання) |

## 7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА


1. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.
3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Изд. «Юниор». -2003. – 504 с. 2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: DiaSoft.–2002. – 688 с.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб: «Наука и Техника». - 2004.- 384 с.
5. Ларс Кландер. Hacker Proof: Полное руководство по безопасности компьютера. – Минск: «Попурри». -2002.- 688 с.
6. Эндрю Локхард. Антихакинг в сети. Трюки. – СПб: «Питер». - 2005.- 295 с.
7. Богуш В.М. Інформаційна безпека держави: навч. посіб./В.М. Богуш, О.К. Юдін – К.: «МК-Прес», 2005. – 432 с. 2. Столлингс Вильям. Криптографическая защита сетей/Столлингс Вильям – М.: Изд. дом “Вильямс”, 2001.
8. Домарев В.В. Защита информации и безопасность компьютерных систем/ Домарев В.В. – К.: Диа-софт, 1999.
9. Богуш В.М. Інформаційна безпека: Термінологічний навчальний довідник/ Богуш В.М., Кривуца В.Г., Кудін А.М.; за ред. Кривуци В.Р. – К.:ООО "Д.В.К.", 2004. – 508 с.
10. Єфремов В.П. Технічна експлуатація систем захисту інформації. Част. 2. Експлуатація безпечних інформаційних технологій: навч. посіб./ Єфремов В.П., Кононович В.Г., Тардаскін М.Ф.; за ред. М.В. Захарченка. – Одеса: ОНАЗ, 2003. – С. 248.

11. Тардаскін М.Ф. Технічний захист комерційної таємниці підприємства зв'язку: навч. посіб.; / за ред. М.В. Захарченка / М.Ф. Тардаскін, В.Г. Кононович / – Одеса: ОНАЗ, 2002. – 76 с

**Нормативно-правова база**

1. Закон України "Про захист персональних даних".
2. Закон України "Про інформацію".
3. Закон України "Про доступ до публічної інформації".
4. Закон України "Про захист інформації в інформаційно-телекомуніка-ційних системах".
5. Закон України "Про телекомунікації".
6. Закон України "Про ліцензування видів господарської діяльності".
7. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 № 1126.
8. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення".
9. Постанова Кабінету Міністрів України від 29.10.00 № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".
10. Постанова Кабінету Міністрів України від 16.11.2016 № 821 "Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України".
11. Постанова Кабінету Міністрів України від 21.06.17 № 437 "Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації".
12. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
13. Постанова Кабінету Міністрів України від 13.03.02 № 281 "Про деякі питання захисту інформації, охорона якої забезпечується державою".
14. Постанова Кабінету Міністрів України від 29.03.06 № 373 "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".
15. Постанова Кабінету Міністрів України від 12.04.02 № 522 "Порядок підключення до глобальних мереж передачі даних".
16. Положення про порядок надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців, затверджено Наказом Державного комітету України з питань регуляторної політики та

підприємництва 20.10.2005 № 97, Зареєстровано в Міністерстві юстиції України 28 жовтня 2005 р. за № 1294/11574.
17. Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 № 93, зареєстровано в Міністерстві юстиції України 16.07.07 за № 820/14087.
18. Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.07 № 87, зареєстровано в Міністерстві юстиції України 10.07.07 за № 785/14052.
19. Правила проведення робіт із сертифікації засобів захисту інформації, затверджені наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.07 № 75/91 та зареєстровані у Мін`юсті 14.05.07 № 498/13765.
20. Порядок формування реєстру організаторів державної експертизи у сфері технічного захисту інформації та реєстру експертів з питань технічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.04.08 № 64.
21. Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 26.03.07 № 45.
22. Тимчасове положення про категоріювання об'єктів від 10.07.95 № 35.
23. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
24. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
25. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
26. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
27. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
28. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
29. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації захисту інформації в комп'ютерних системах від несанкціонованого доступу.
30. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
31. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
32. НД ТЗІ 2.5-010-2003 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу.
33. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та

модернізації засобів технічного захисту інформації від несанкціонованого доступу.
34. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною № 1, затвердженою наказом ДСТСЗІ СБ україни 18.06.02 № 37).
35. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
36. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
37. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
38. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
39. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

## 8. ПЕРЕЛІК ПИТАНЬ ДО ЕКЗАМЕНУ

1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням.
2. Положення про державну експертизу в сфері технічного захисту інформації.
3. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
4. Порядок проведення перед проектних досліджень на об'єкті інформаційної діяльності.
5. Рекомендації щодо розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності.
6. Система технічного захисту інформації в Україні: стан та напрями розвитку.
7. Перехоплення даних.
8. Класифікація каналів витоку інформації.
9. Технічні канали витоку інформації.
10. Методи за засоби захисту від витоку інформації.
11. Поняття інженерно-технічного захисту.
12. Фізичні засоби захисту: охоронні системи.
13. Фізичні засоби захисту: охоронне телебачення.
14. Фізичні засоби захисту: охоронне освітлення.

15. Фізичні засоби захисту: засоби охоронної сигналізації.
16. Апаратні засоби захисту.
17. Ключові елементи: ключові дискети, USB- та LPT-ключі.
18. Персональні кодові карти.
19. Персональний ідентифікатор.
20. Пристрої розпізнавання голосу користувача чи форми його пальців.
21. Класифікація закладних пристроїв.
22. Основні характеристики закладних пристроїв.
23. Застосування закладних пристроїв.
24. Пристрої для захисту інформації у мережах.
25. Класи безпеки інформаційних систем.
26. Загрози безпеці інформації.
27. Основні поняття та класифікація загроз.
28. Порушники інформаційної безпеки, їх класифікація.
29. Модель поводження потенційного порушника.
30. Критерії оцінювання безпеки інформаційних технологій.
31. Моделі управління доступом.
32. Моніторинг ринку України на наявність приладів для захисту інформації.
33. Апаратні засоби захисту в мережах.