МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Юридичний факультет
Кафедра кримінального правосуддя та правоохоронної діяльності

СИЛАБУС
вибіркового освітнього компонента

ОСНОВИ КІБЕРЗАХИСТУ В ПРАВООХОРОННИХ ОРГАНАХ

підготовки бакалавра

Луцьк – 2025

Силабус вибіркового освітнього компонента «Основи кіберзахисту в правоохоронних органах» підготовки бакалавра

Розробник: Бендовський Григорій Валерійович, старший викладач кафедри кримінального правосуддя та правоохоронної діяльності юридичного факультету Волинського національного університету імені Лесі Українки

Погоджено
Гарант освітньо-професійної програми:
_____ (к.ю.н., доц. Фідря Ю. О.)

Силабус нормативного освітнього компонента затверджено на засіданні кафедри кримінального правосуддя та правоохоронної діяльності
протокол № 01 від 29 серпня 2025 р.

Завідувач кафедри:_____ (к.ю.н., доц. Фідря Ю. О.)

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна (очна) форма навчання</td><td rowspan="8">Галузь знань
26 Цивільна безпека,

спеціальність
262 Правоохоронна діяльність,

освітньо-професійна програма
Правоохоронна діяльність

освітній рівень:
перший (бакалаврський</td><td>Вибіркова 7</td></tr>
<tr><td>Рік навчання 3-й</td></tr>
<tr><td rowspan="3">Кількість годин/кредитів 120/4</td><td>Семестр 5-ий</td></tr>
<tr><td>Лекції 28 год.</td></tr>
<tr><td>Практичні (семінарські) 28 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Самостійна робота 56 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання Українська</td><td></td></tr>
</table>

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна (очна) форма навчання</td><td rowspan="8">Галузь знань
26 Цивільна безпека,

спеціальність
262 Правоохоронна діяльність,

освітньо-професійна програма
Правоохоронна діяльність

освітній рівень:
перший (бакалаврський</td><td>Вибіркова 7</td></tr>
<tr><td>Рік навчання 3-й</td></tr>
<tr><td rowspan="3">Кількість годин/кредитів 120/4</td><td>Семестр 5-ий</td></tr>
<tr><td>Лекції 6 год.</td></tr>
<tr><td>Практичні (семінарські) 10 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Самостійна робота 90 год.</td></tr>
<tr><td>Консультації 14 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання Українська</td><td></td></tr>
</table>

ІІ. Інформація про викладача

ПІП Бендовський Григорій Валерійович
Посада старший викладач кафедри кримінального правосуддя та правоохоронної діяльності
Контактна інформація 0505501511, Bendovskyi.Hryhorii@vnu.edu.ua
Дні занять: http://194.44.187.20/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

1. Анотація освітнього компонента

Програма освітнього компонента спрямована на формування у здобувачів освіти базових знань механізму безпеки при роботі з комп'ютером, основних засад кібербезпеки на робочому місці та в повсякденному житті, використання сучасних комп'ютерно-інформаційних технологій, а також забезпечити формування інформаційної культури та набуття практичних навичок для застосування у майбутній професії.

2. Мета і завдання освітнього компонента

Мета цього освітнього компонента полягає в тому, щоб розвивати у здобувачів освіти вміння, які сприяють конкретному та послідовному мисленню, здатність висловлювати свої власні думки, критичне мислення, роботу з різноманітними джерелами та фактичним матеріалом, а також вміння чітко й точно висловлювати свої погляди, аргументувати їх і брати участь в обґрунтованих дискусіях.

Програма цього освітнього компонента сформує необхідні знання щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із компютерної технікою в професійній діяльності. Слухачі дізнаються про основні загрози в сучасному інформаційному просторі, наслідки атак зловмисників та кібершахраїв.

Набуті у ході вивчення освітнього компонента навички підвищать конкурентоспроможність молодих фахівців на ринку праці.

Для досягнення поставленої мети передбачені такі основні завдання:

- знання основних положень. термінів та заходів, що стосуються кібергігієни на робочому місці;
- знання нормативно-правової бази у сфері кібербезпеки;
- уміння оцінювати загрози та вживати заходів реагування на робочому місці;
- уміння безпечно поводитись у кіберпросторі;
- знати методи якими нападники проникають в комп'ютерну систему: соціальна інженерія, злам паролю, фішинг, спуфінг та інше.

3. Результати навчання (Компетентності)

Загальні компетентності (ЗК):

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 7. Здатність до адаптації та дії в новій ситуації.

ЗК 8. Здатність приймати обґрунтовані рішення.

ЗК 12. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

Спеціальні компетентності (СК):

СК 3. Здатність до критичного мислення та системного аналізу правових явищ.

СК 4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК 8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати спеціалізовані інформаційні системи та програмне забезпечення.

СК 9. Здатність надавати правоохоронні послуги.

СК 16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури.

СК 17. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.

Результати навчання (РН):

РН 8. Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для виконання професійних завдань.

РН 9. Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси з метою виконання професійних завдань у сфері правоохоронної діяльності.

РН 14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя.

РН 18. Застосовувати інформаційні системи та технології, технології захисту даних, методи обробки, накопичення та аналізу інформації.

РН 21. Організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.

Під час вивчення освітнього компонента здобувачі набудуть таких soft skills:

- уміння чітко, логічно і стисло формулювати думку;
- здатність усвідомлювати рівні можливості та гендерні проблеми;
- навички активного слухання;
- здатність до критичного мислення та аналізу;
- здатність працювати в умовах обмеженого часу;
- уміння застосовувати норми права в конкретних ситуаціях;
- здатність до комплексної оцінки ситуації та наслідків прийнятих рішень;
- здатність обґрунтовувати юридичні рішення;

- навички побудови юридичних аргументів.

Цьому сприяють такі методи навчання: дискусії, ситуаційний аналіз, мозкові атаки тощо.

4. Структура освітнього компонента

Денна форма навчання

Назви змістових модулів і тем	**Усього**	**Лек.**	**Практ.**	**Сам. роб.**	**Конс.**	**Форма контролю**
Тема 1. Потреба в кібербезпеці. Атаки, поняття та методи.	4	2	2	-	-	ДС+ДБ +УО
Тема 2. Основи забезпечення захисту інформації та кібербезпеки на об'єктах інформаційної діяльності правоохоронних органів України.	4	2	2	-	-	ДС+ДБ +УО
Тема 3. Захист службових даних та інформації з обмежених доступом.	4	2	2	-	-	ДС+УО+ РЗ/К+УО
Тема 4. Основи застосування інформаційно-пошукових систем та мережі Інтернет в правоохоронній діяльності.	4	2	2	-	-	
Тема 5. Загальні принципи використання державних реєстрів та відомчих інформаційних систем при здійсненні інформаційно-аналітичній діяльності правоохоронними органами.	4	2	2	-	-	

Тема 6. Загальний порядок використання сучасного програмного забезпечення для обробки та аналізу здобутої оперативної інформації.	4	2	2	-	-	
Тема 7. Реагування на інциденти інформаційної безпеки.	4	2	2	-	-	
Всього годин/Балів	**120**	**28**	**28**	**56**	**8**	

Заочна форма навчання

Назви змістових модулів і тем	**Усього**	**Лек.**	**Практ.**	**Сам. роб.**	**Конс.**	**Форма контролю**
Тема 1. Потреба в кібербезпеці. Атаки, поняття та методи.	4	2	2	-	-	ДС+ДБ +УО
Тема 2. Основи забезпечення захисту інформації та кібербезпеки на об’єктах інформаційної діяльності правоохоронних органів України.	4	2	2	-	-	ДС+ДБ +УО
Тема 3. Захист службових даних та інформації з обмежених доступом.	4	2	2	-	-	ДС+УО+ РЗ/К+УО
Тема 4. Основи застосування інформаційно-пошукових систем та мережі Інтернет в правоохоронній діяльності.	4	2	2	-	-	
Тема 5. Загальні принципи використання державних реєстрів та відомчих інформаційних систем	4	2	2	-	-	

при здійсненні інформаційно-аналітичній діяльності правоохоронними органами.						
Тема 6. Загальний порядок використання сучасного програмного забезпечення для обробки та аналізу здобутої оперативної інформації.	4	2	2	-	-	
Тема 7. Реагування на інциденти інформаційної безпеки.	4	2	2	-	-	
Всього годин/Балів	**120**	**6**	**10**	**90**	**14**	

*Методи контролю: ДС – дискусія, ДБ – дебати, Т – тести, РЗ/К – розв'язування задач/кейсів, УО – усне опитування.
**Порядок нарахування балів за поточний контроль див. у розділі «Політика оцінювання»

При вивченні ВОК використовуються:

Дидактичні методи - лекції з використанням мультимедійних презентацій.

Практичні методи: практичні заняття з використанням прикладного програмного забезпечення.

Метод самостійного навчання.

Активні методи: експрес опитування, тестування.

Словесні методи навчання: лекції, консультації.

Технічне й програмне забезпечення /обладнання.

Комп'ютери, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word), вільне програмне забезпечення (GNU General Public License), електронне освітнє середовище - Віртуальний університет (на базі платформи Moodle).

Інформаційний обсяг освітнього компонента

Тема 1. Потреба в кібербезпеці. Атаки, поняття та методи. Основні поняття про захист інформації на об'єктах інформаційної діяльності. Основні поняття про технічні канали витоку інформації на об'єктах інформаційної діяльності. Основні методи блокування та приховування витоку інформації технічними каналами

Тема 2. Основи забезпечення захисту інформації та кібербезпеки на об'єктах інформаційної діяльності правоохоронних органах України. Основні поняття про інформаційно-пошукову та аналітичну роботу, технології ILP (англ. – Intelligence Led Policing, поліцейська діяльність керована аналітикою). Основні поняття про стратегічний, оперативний та

тактичний кримінальний аналіз. Основні поняття про захист інформації на об'єктах інформаційної діяльності.

Тема 3. Захист службових даних та інформації з обмежених доступом. Основні поняття про технічні канали витоку інформації на об'єктах інформаційної діяльності. Основні методи блокування та приховування витоку інформації технічними каналами. Основні поняття про організацію та забезпечення технічного захисту інформації на об'єктах інформаційної діяльності правоохоронних органів України.

Тема 4. Основи застосування інформаційно-пошукових систем та мережі Інтернет в правоохоронній діяльності. Захист даних і конфіденційність. Шифрування та знищення даних. Захист персонального комп'ютера. Безпечне використання USB. Основи застосування технології інтелект-карт для систематизації здобутих з мережі Інтернет базових відомостей стосовно об'єкту зацікавленості досудового розслідування.

Тема 5. Загальні принципи використання державних реєстрів та відомчих інформаційних систем при здійсненні інформаційно-аналітичній діяльності правоохоронними органами. Джерела інформації, що використовуються підрозділами кримінальної поліції для обробки та аналізу криміналістичної інформації можливостями програмних продуктів офісного пакету Microsoft Office та ШІ Analyst's Notebook. Загальний порядок пошуку, обробки та аналізу інформації з:

– Реєстру речових прав на нерухоме майно Міністерства юстиції України;

– інтегрованої інформаційно-комунікаційної системи «Аркан» Державної прикордонної служби України;

– телефонного трафіку;

– інформаційно-аналітичного комплексу «Безпечне місто»;

– реєстрів Державної податкової служби України;

– банківських установ, електронних платіжних систем та систем онлайн-банкінгу тощо.

Тема 6. Загальний порядок використання сучасного програмного забезпечення для обробки та аналізу здобутої оперативної інформації. Основні можливості програмних продуктів Word, Excel з офісного пакету Microsoft Office як засобів обробки та аналізу криміналістичної інформації. Основні можливості аналітичного програмного продукту ШІ Analyst's Notebook. Джерела інформації, що використовуються підрозділами кримінальної поліції для обробки та аналізу оперативної інформації можливостями програмних продуктів офісного пакету Microsoft Office та ШІ Analyst's Notebook. Інші програмні продукти, що можуть використовуватися для обробки та аналізу криміналістичної інформації під час досудового розслідування кримінальних правопорушень.

Тема 7. Реагування на інциденти інформаційної безпеки. Система управління інформаційною безпекою. Процедури реагування на інциденти інформаційної безпеки. Правові аспекти та політики цифрової безпеки. Політика України в галузі кібергігієни.

5. Завдання для самостійного опрацювання.

Самостійна робота передбачає опрацювання теоретичних основ лекційного матеріалу по кожній темі та виконання завдань і оцінюється викладачем індивідуально відповідно до шкали оцінювання.

IV. Політика оцінювання

Відповідно до Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки від 26 червня 2025 р. протокол № 8 Вченої ради (https://vnu-taskid841251.s3.eu-north-1.amazonaws.com/s3fs-public/inline-files/2025-pro-potochne-i-pidsumk.otsinyuvannya.pdf) поточний контроль здійснюється під час проведення практичних занять і має за мету перевірку рівня підготовленості здобувачів освіти до виконання конкретної роботи та реалізується в різних формах, зокрема опитування, виступи на практичних заняттях, заслуховування та аналіз доповідей питань, винесених на обговорення, письмове вирішення завдань, письмові відповіді на окремі питання, участь у дискусіях/дебатах, перевірка результатів виконання різноманітних індивідуальних завдань, контроль засвоєння того навчального матеріалу, який заплановано на самостійне опрацювання здобувачем, тощо.

Максимальна кількість балів за поточний контроль – 100 балів.

Політика викладача щодо здобувача освіти:

- обов'язкове відвідування навчальних занять;
- активність здобувача освіти під час занять;
- своєчасне виконання завдань/робіт, щодо яких встановлено дедлайни.

Не допускається:

- ✓пропуск занять без поважних причин;
- ✓систематичні запізнення на заняття;
- ✓користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (за винятком дозволу викладача при зверненні до текстів нормативних актів та в інших навчальних цілях).

Політика щодо академічної доброчесності

Вивчаючи цей ОК, здобувач освіти погоджується виконувати етичні принципи та визначені законом правила, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Здобувач освіти зобов'язаний дотримуватись політики академічної доброчесності, що передбачає:

• самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми

потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

• посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

• дотримання норм законодавства про авторське право і суміжні права;

• надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Основні засади дотримання академічної доброчесності визначено у Положенні про систему запобігання та виявлення академічного плагіату в науковій та навчальній діяльності здобувачів вищої освіти, докторантів, науково-педагогічних і наукових працівників Волинського національного університету імені Лесі Українки https://ra.vnu.edu.ua/wp-content/uploads/2025/02/Polozhennya-pro-plagiat-gruden-24.pdf, а також у Кодексі академічної доброчесності Волинського національного університету імені Лесі Українки https://ra.vnu.edu.ua/wp-content/uploads/2023/06/Kodeks-akademichnoyi-dobrochesnosti.pdf

Політика щодо дедлайнів та перескладання.

Пропущені практичні заняття (незалежно від поважності причини) перескладаються шляхом виконання завдань практичного заняття. За результатами перездачі виставляється оцінка відповідно до шкали оцінювання роботи здобувача освіти на практичних заняттях.

Пропуски на практичних заняттях та негативні оцінки (0 балів) можуть бути перескладені до початку заліково-екзаменаційної сесії відповідно до графіку чергування викладача, затвердженого на кафедрі.

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті.

Визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, здійснюється на добровільній основі та передбачає підтвердження того, що здобувач освіти досяг результатів навчання, передбачених ОП, за якою він навчається. Визнанню можуть підлягати такі результати навчання, отримані в неформальній освіті, які за тематикою, обсягом вивчення та змістом відповідають як ОК в цілому, так і його окремому розділу, темі (темам), індивідуальному завданню, контрольній роботі тощо, які передбачені силабусом ОК (Порядок визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки від 29 серпня 2024 року https://ed.vnu.edu.ua/wp-content/uploads/2024/09/2024_%D0%92%D0%B8%D0%B7%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F_%D1%80%D0%B5%D0%B7%D1%83%D0%BB_%D1%82%D0%B0%D1%82i%D0%B2_%D0%92%D0%9D%D0%A3_i%D0%BC._%D0%9B.%D0%A3._%D1%80%D0%B5%D0%B4.pdf)

Неформальна освіта з запобігання та протидії насильству охоплює тренінги й воркшопи, програми громадських і міжнародних організацій, онлайн-курси. Здобувачі можуть проходити відкриті курси з кібербезпеці на

платформах Prometheus, HELP Ради Європи (Human Rights Education for Legal Professionals). Рекомендовано пройти такі курси:

Можливість отримати додаткові (бонусні) бали.

Відповідно до п 4.5. вищезазначеного Положення передбачено, що здобувачам освіти, які брали участь у роботі конференцій, підготовці наукових публікацій, в олімпіадах, конкурсах студентських наукових робіт тощо й досягли значних результатів, може бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю з відповідного ОК.

Науково-методичною комісією факультету затверджено систему бонусних балів, які зараховуються як результати поточного контролю з відповідного ОК в обсязі до 35 балів (протокол № 01 від 03 вересня 2025 р.).

Види студентської наукової та практичної активності	**Кількість бонусних балів**
Публікація наукової статті в періодичному науковому фаховому виданні категорії «Б» (у співавторстві із науковим керівником)	до 7 балів
Виступ з доповіддю на міжнародній, всеукраїнській науково-практичній конференції, засіданні круглого столу, симпозіуму та іншому науковому заході	до 5 балів
Публікація тез доповіді у збірнику матеріалів конференції, круглого столу чи іншого наукового заходу	до 5 балів
Участь у Всеукраїнській студентській олімпіаді	до 8 балів
Участь у Всеукраїнському конкурсі студентських наукових робіт	до 10 балів

V. Підсумковий контроль

Згідно Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки від 26 червня 2025 року (URL: https://vnu-taskid841251.s3.eu-north-1.amazonaws.com/s3fs-public/inline-files/2025-pro-potochne-i-pidsumk.otsinyuvannya.pdf) підсумковий контроль проводиться з метою оцінки результатів навчання на певному освітньому рівні або на окремих його завершальних етапах у формі заліку.

Залік викладач виставляє за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом ОК. У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

Залік виставляється за результатами поточної роботи здобувача освіти без планування, проведення модульних контрольних робіт (оцінювання за шкалою від 0 до 100). Мінімальна позитивна кількість балів – 60.

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше

як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості 100.

У день складання заліку за основною сесією не проводяться додаткові опитування здобувача освіти, а також здобувач освіти не має права доздавати будь-який вид робіт, передбачений силабусом освітнього компоненту.

Повторне складання заліку допускається не більше як два рази: один раз – викладачеві, другий – комісії, яку створює декан факультету.

Залік проводиться в очній формі.

Перелік питань на залік

VI. Шкала оцінювання

Оцінка в балах	Лінгвістична оцінка
90 – 100	Зараховано
82 – 89	
75 - 81	
67 -74	
60 - 66	
1 – 59	Незараховано (необхідне перескладання)

90-100 – здобувач освіти демонструє вільне володіння теоретичними питаннями, вміє переконливо, з посиланням на законодавство обґрунтовувати проблему, яку висвітлює; безпомилково дає відповіді на поставлені питання з посиланням на норми законодавства; вільно володіє термінологією;

82-89 – здобувач освіти при відповіді на теоретичні питання відповідає повно, володіє термінологією, знає нормативно-правові акти, вміло їх застосовує при відповіді на питання, однак може допускати деякі неточності чи положення без їх доведеності;

75-81 – здобувач освіти при відповіді на теоретичні питання може порушувати системність їх викладу, допускати окремі неточності, без їх доказовості, однак знає нормативно-правові акти, застосовує при відповіді на питання, володіє основними категоріями;

67-74 – здобувач освіти володіє більшістю теоретичними питаннями з предмету вивчення, володіє термінологією, знає нормативно-правові акти; однак не завжди може правильно та аргументовано застосувати норми законодавства;

60-66 – здобувач освіти не володіє більшістю теоретичними питаннями, однак знає основні категорії та нормативно-правові акти, але при відповіді на питання не обґрунтовує та не аргументує свою відповідь;

1-59 – здобувач освіти володіє теоретичними питаннями поверхнево; знає окремі категорії та нормативно-правові акти, але не вміє правильно їх застосовувати під час відповіді на питання.

балів / балів – поточне оцінювання (денна/заочна форма навчання)

№ п/п	бали	Оцінка	Оцінка відповідно ECES
1		**відмінно**	здобувач освіти демонструє вільне володіння питаннями практичного заняття, вміє переконливо, з посиланням на норми законодавства обґрунтовувати проблему, яку висвітлює; безпомилково виконує практичні завдання, бере участь у дискусії;
2		**добре**	здобувач освіти при відповіді на теоретичні питання практичного заняття допускає поодинокі неточності, однак знає нормативно-правові акти, вміє їх застосовувати під час розв'язуванні задач (кейсів) та аргументувати свою відповідь;
3		**задовільно**	здобувач освіти не володіє більшістю питань практичного заняття, однак знає нормативно-правові акти; виконуючи завдання, посилається на законодавство, але не обґрунтовує свою відповідь;
4		**незадовільно**	здобувач освіти володіє питаннями практичного заняття поверхнево; знає нормативно-правові акти, але не вміє правильно застосовувати під час розв'язування практичних завдань.

балів / балів – оцінювання самостійної роботи (у розділі самостійна робота написано, що вона оцінюється згідно шкали) (денна/заочна форма навчання)

№ п/п	бали	Оцінка	Оцінка відповідно ECES
1		**відмінно**	здобувач освіти демонструє вільне володіння питаннями практичного заняття, вміє переконливо, з посиланням на норми законодавства обґрунтовувати проблему, яку висвітлює; безпомилково виконує практичні завдання, бере участь у дискусії;
2		**добре**	здобувач освіти при відповіді на теоретичні питання практичного заняття допускає поодинокі неточності, однак знає нормативно-правові акти, вміє їх застосовувати під час розв'язуванні задач (кейсів) та аргументувати свою відповідь;
3		**задовільно**	здобувач освіти не володіє більшістю питань практичного заняття, однак знає нормативно-правові акти; виконуючи завдання, посилається на законодавство, але не обґрунтовує свою відповідь;
4		**незадовільно**	здобувач освіти володіє питаннями практичного заняття поверхнево; знає нормативно-правові акти,

			але не вміє правильно застосовувати під час розв’язування практичних завдань.

VII. Рекомендована література та Інтернет-ресурси

Навчальна та наукова література

Основна

1. Безпека інформаційних систем: навч. пос. / В. І. Пашорін, Ю. В. Костюк. Київ: Держ. торг.-екон. ун-т, 2022. 376 с.
2. Гребенюк А.М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. пос. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Когут Ю. Кібервійна та безпека об’єктів критичної інфраструктури. К., 2021. 332 с.
4. Основи кібербезпеки та кібероборони: підруч. / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. [видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О. С. Попова, 2019. 320 с. ISBN 978-617-582-069-8
5. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. К.: Видавництво Ліра-К, 2020. 554 с.

Додаткова

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

Інтернет ресурси

1. Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак - https://osvita.diia.gov.ua/courses/cyber-hygiene
2. Цифрова безпека для громадських організацій в умовах війни - https://prometheus.org.ua/course/course-v1:Prometheus+DSPO101+2023_T1?utm_source=sendy&utm_medium=email&utm_campaign=email-aprildigest23-digital security