ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних
технологій
28 серпня 2024 р., протокол № 8
Голова Вченої ради

Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Основи захисту інформації»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 256 «Національна безпека
(за окремими сферами забезпечення і видами діяльності»
освітньо-професійна програма «Національна безпека
(за окремими сферами забезпечення і видами діяльності»
факультет національної безпеки, права та міжнародних відносин
кафедра національної безпеки, публічного управління та адміністрування

Схвалено на засіданні кафедри
інженерії програмного
забезпечення
28 серпня 2024 р.,
протокол № 7

Завідувач кафедри
Тетяна ВАКАЛЮК

Гарант освітньої-професійної програми
Ірина СУПРУНОВА

Розробник: к.тех.н., доц., доцент кафедри інженерії програмного забезпечення
Надія ЛОБАНЧИКОВА

Житомир
2024

Робоча програма навчальної дисципліни «Основи захисту інформації» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» за освітньо-професійною програмою «Національна безпека (за окремими сферами забезпечення і видами діяльності)» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
25 «Воєнні науки, національна безпека, безпека державного кордону»</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">Спеціальність
256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 1</td><td colspan="2">3</td></tr>
<tr><td>Загальна кількість годин – 120</td><td colspan="2">Семестр</td></tr>
<tr><td></td><td colspan="2">6</td></tr>
<tr><td rowspan="9">Тижневих годин для денної форми навчання:
аудиторних – 4</td><td rowspan="9">Освітній ступінь «бакалавр»</td><td colspan="2">Лекції</td></tr>
<tr><td>32 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>32 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>104 год.</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання – 13 % аудиторних занять, 87 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти основних знань та положень з принципів та основ захисту інформації в інфо-телекомунікаційних мережах і системах, набуття вмінь та навичок щодо формування політики інформаційної безпеки телекомунікаційних систем, методи забезпечення інформаційної безпеки та управління ризиками у кіберпросторі, а також розвиток навичок використання цифрових інструментів для аналізу, прогнозування і протидії кіберзагрозам у контексті національної безпеки.

Завданнями вивчення навчальної дисципліни є набуття знань щодо:

–формування теоретичної бази, практичних навиків, які необхідні для фахівця організовувати систему захисту інформації в сучасних інфотелекомунікаційних системах, вміти організовувати заходи щодо протидії злочинним діям, спрямованим на втрату, заміну, підробку інформації або виведення (часткового чи повного) із режиму нормальної роботи обладнання;

–розвинути навички застосування сучасних інформаційних технологій у забезпеченні кібербезпеки, прогнозуванні загроз і побудові стратегій захисту.

Зміст навчальної дисципліни спрямований на формування наступних **компетентностей** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК 13. Здатність виявляти можливі загрози інформаційному простору та протидіяти інформаційно-психологічним впливам шляхом використання інформаційно-комунікаційних технологій, імплементації сучасних методів інформаційної безпеки та захисту інформації.

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів навчання** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.

ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати наступні Soft skills:

– *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;

– *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;

– *керування часом:* уміння справлятися із завданнями вчасно;

– *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

– *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;

– *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основи кібербезпеки та захисту інформації

Тема 1. Загальні положення про інформаційні ресурси (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6)

Інформаційні ресурси: поняття, зміст. Загальна характеристика національних інформаційних ресурсів. Інформаційні ресурси організацій. Режим доступу до інформації. Поняття персональних даних, правова основа їх захисту. Електронний документообіг та його безпека: цифровий підпис, шифрування документів. Роль інформаційних ресурсів у національній безпеці: критична інформаційна інфраструктура, державні реєстри.

Тема 2. Сучасні загрози мережевої безпеки (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Забезпечення безпеки мереж. Мережеві загрози. Нейтралізація загроз. Перехоплювачі паролів першого роду. Перехоплювачі паролів другого роду. Перехоплювачі паролів третього роду. Принципи роботи троянських програм. Принципи роботи утиліт скритого адміністрування Комп’ютерні віруси і механізми боротьби з ними Класифікація комп’ютерних вірусів. Методи і засоби боротьби з вірусами. Пакетні фільтри

Тема 3. Забезпечення безпеки мережевих пристроїв (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Захист доступу до пристроїв. Призначення адміністративних ролей. Моніторинг пристроїв і керування ними. Використання автоматичних функцій забезпечення безпеки. Захист у площині управління. Використання міжмережевих екранів. Політика безпеки під час роботи в мережі

Тема 4. Аутентифікація, авторизація та облік (ЗК 1, ЗК 5, СК 13, ПРН 6)

Призначення AAA. Локальна аутентифікація AAA. Серверна аутентифікація

ААА. Серверна авторизація та облік. Порівняння методів аутентифікації: використання OAuth, OpenID, SAMLy сучасній системі. Журнали безпеки та аудит дій користувачів: логування та моніторинг подій. Захист від атак: фішинг, кейлогери, атаки на відновлення пароля.

Тема 5. Впровадження технологій брандмауера (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Списки контролю доступу. Технології брандмауера. Зональні міжмережеві екрани. Види брендмауерів: мережеві, хмарні, персональні. Порівняння статичних та динамічних фаєрволів. Конфігурація брандмауера для різних рівнів безпеки. Захист від DoS та DDoS-атаки за допомогою брендмауерів.

Тема 6. Впровадження системи запобігання вторгнень (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Технології IPS. Сигнатури IPS. Впровадження системи IPS. Відмінності між системою виявлення вторгнень (IDS) та системою запобігання вторгненням (IPS). Використання SNORT, Suricata, Zeek (Bro) для виявлення вторгнення. Підходи до аналізу трафіку: сигнатурний поведінковий аналіз. Методи обходу системи вторгнення та способи їхнього захисту. Інтеграція IPS/IDS із SIEM-системами для централізованого моніторингу.

Тема 7. Забезпечення безпеки локальної мережі (LAN) (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Безпека кінцевих пристроїв. Загрози безпеці на 2-му рівні. Комплексна політика безпеки. Фізична безпека мережевого обладнання та контролю доступу. Використання VLAN (Virtual LAN) для ізоляції трафіку. Захист від атак ARP-спуфінгу, MAC-затоплення, голодування DHCP. Поняття керування доступом до мережі (NAC) та його роль у безпеці LAN.

Тема 8. Криптографічні системи (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Криптографічні сервіси. Базові відомості про цілісність і аутентифікації. Конфіденційність. Криптографія з відкритими ключами. Класифікація та вимоги до сучасних криптосистем.

Тема 9. Впровадження віртуальних приватних мереж (VPN) (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Сеті VPN. Компоненти і принципи роботи IPsec VPN. Впровадження мереж IPsec VPN за схемою Site-to-Site (VPN між двома пунктами) з використанням інтерфейсу командного рядка (CLI). Типи VPN: Remote Access VPN, Intranet VPN, Extranet VPN. Порівняння IPsec VPNта SSL VPN. Використання OpenVPN таWireGuardy. Захист VPN: шифрування трафіку, аутентифікація користувачів, управління ключами.

Тема 10. Захист інформації на мережевому рівні (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

Міжмережеві екрани. Протокол мережевої безпеки IPSec. Протокол SSL. Протокол TLS. Аналіз вразливостей у IPsec, SSL та TLS. Роль сертифікатів безпеки у захист. Використання глибокої перевірки пакетів (DPI)у мережі. Захист трафіку від атак MITM (Man-In-The-Middle)

Тема 11. Захист бездротових мереж (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 13)

WEP. WPA. TKIP. PSK. WPA2 Personal.WPA3. Основні атаки бездротової мережі: Evil Twin, KRACK, Deauthentication Attack. Методи підбору паролів та захисту від атаки грубою силою. Порівняння WPA2 vs WPA3. Використання MAC-фільтрації та прихованих SSID

Тема 12. Технічні канали просочування інформації (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6)

Акустичний канал, віброакустичний канал, гідроакустичний канал, акустоелектричний канал, електромагнітний канал. Методи виявлення витоків інформації через технічні канали. Використання екранування та фільтрації сигналів для захисту. Захист від електромагнітного випромінювання (TEMPEST). Методи акустомаскування та захисту від підслуховування

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	самостійна робота	усього	лекції	практичні	самостійна робота
Змістовий модуль 1. Основи кібербезпеки та захисту інформації								
Тема 1. Загальні положення про інформаційні ресурси	4	2	–	2	4	1	–	3
Тема 2. Сучасні загрози мережевої безпеки	6	2	2	2	6	1	-	5
Тема 3. Забезпечення безпеки мережевих пристроїв	12	4	4	4	12	1	-	11
Тема 4. Аутентифікація, авторизація та облік	12	4	4	4	12	1	1	10
Тема 5. Впровадження технологій брандмауера	12	2	4	6	12	1	1	10
Тема 6. Впровадження системи запобігання вторгнень	8	2	2	4	8	1	1	6
Тема 7. Забезпечення безпеки локальної мережі (LAN)	14	4	4	6	14	1	1	12
Тема 8. Криптографічні системи	14	4	4	6	14	1	1	12
Тема 9. Впровадження віртуальних приватних мереж (VPN)	12	2	4	6	12	1	1	10
Тема 10. Захист інформації на мережевому рівні	8	2	–	6	8	1	–	7
Тема 11. Захист бездротових мереж	10	2	2	6	10	-	-	10
Тема 12. Технічні канали просочування інформації	7	2	1	4	7	-	-	7
Модульний контроль	1	-	1	-	-	-	-	-
ВСЬОГО	**120**	**32**	**32**	**56**	**120**	**10**	**6**	**104**

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 2.** Сучасні загрози мережевої безпеки	2	–
2	**Тема 3.** Забезпечення безпеки мережевих пристроїв	4	-
3	**Тема 4.** Аутентифікація, авторизація та облік	4	-
4	**Тема 5.** Впровадження технологій брандмауера	4	1
5	**Тема 6.** Впровадження системи запобігання вторгнень	2	1
6	**Тема 7.** Забезпечення безпеки локальної мережі (LAN)	4	1
7	**Тема 8.** Криптографічні системи	4	1
8	**Тема 9.** Впровадження віртуальних приватних мереж (VPN)	4	1
9	**Тема 11.** Захист бездротових мереж	2	1
10	**Тема 12.** Технічні канали просочування інформації	1	–
11	Модульний контроль	1	-
РАЗОМ		**32**	**6**

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Загальні положення про інформаційні ресурси Електронний документообіг та його безпека: цифровий підпис, шифрування документів. Роль інформаційних ресурсів у національній безпеці: критична інформаційна інфраструктура, державні реєстри.	2	3
2	**Тема 2.** Сучасні загрози мережевої безпеки Перехоплювачі паролів першого роду. Перехоплювачі паролів другого роду. Перехоплювачі паролів третього роду. Принципи роботи троянських програм. Принципи роботи утиліт скритого адміністрування. Комп'ютерні віруси і механізми боротьби з ними Класифікація комп'ютерних вірусів. Методи і засоби боротьби з вірусами. Пакетні фільтри.	2	5
3	**Тема 3.** Забезпечення безпеки мережевих пристроїв Використання міжмережевих екранів. Політика безпеки під час роботи в мережі	4	11
4	**Тема 4.** Аутентифікація, авторизація та облік Порівняння методів аутентифікації: використання OAuth, OpenID, SAMLy сучасній системі. Журнали безпеки та аудит дій користувачів: логування та моніторинг подій. Захист від атак: фішинг, кейлогери, атаки на відновлення пароля.	4	10
5	**Тема 5.** Впровадження технологій брандмауера Порівняння статичних та динамічних фаєрволів. Конфігурація брандмауера для різних рівнів безпеки. Захист від DoS та DDoS-атаки за допомогою брендмауерів.	6	10
6	**Тема 6.** Впровадження системи запобігання вторгнень Використання SNORT, Suricata, Zeek (Bro) для виявлення вторгнення. Підходи до аналізу трафіку: сигнатурний поведінковий аналіз. Методи обходу системи вторгнення та способи їхнього захисту. Інтеграція IPS/IDS із SIEM-системами для	4	6

	централізованого моніторингу.		
7	**Тема 7.** Забезпечення безпеки локальної мережі (LAN) Використання VLAN (Virtual LAN) для ізоляції трафіку. Захист від атак ARP-спуфінгу, MAC-затоплення, голодування DHCP. Поняття керування доступом до мережі (NAC) та його роль у безпеці LAN.	6	12
8	**Тема 8.** Криптографічні системи Класифікація та вимоги до сучасних криптосистем	6	12
9	**Тема 9.** Впровадження віртуальних приватних мереж (VPN) Типи VPN: Remote Access VPN, Intranet VPN, Extranet VPN. Порівняння IPsec VPNта SSL VPN. Використання OpenVPN таWireGuardy. Захист VPN: шифрування трафіку, аутентифікація користувачів, управління ключами.	6	10
10	**Тема 10.** Захист інформації на мережевому рівні Аналіз вразливостей у IPsec, SSL та TLS. Роль сертифікатів безпеки у захист. Використання глибокої перевірки пакетів (DPI)у мережі. Захист трафіку від атак MITM (Man-In-The-Middle)	6	7
11	**Тема 11.** Захист бездротових мереж Основні атаки бездротової мережі: Evil Twin, KRACK, Deauthentication Attack. Методи підбору паролів та захисту від атаки грубою силою. Порівняння WPA2 vs WPA3. Використання MAC-фільтрації та прихованих SSID	6	10
12	**Тема 12.** Технічні канали просочування інформації Методи виявлення витоків інформації через технічні канали. Використання екранування та фільтрації сигналів для захисту. Захист від електромагнітного випромінювання (TEMPEST). Методи акустомаскування та захисту від підслуховування	4	7
РАЗОМ		**56**	**104**

7. Індивідуальні самостійні завдання

1. Аналіз інформаційних ресурсів України. Дослідити ролі національних інформаційних ресурсів у забезпеченні національної безпеки України. Студентам необхідно охарактеризувати основні категорії національних інформаційних ресурсів, застосовувати їх значення для безпеки держави, зокрема для критичної інфраструктури та державних реєстрів. Важливо відзначити, які з цих ресурсів є особливо вразливими до кіберзагроз і потребують підвищеного захисту. Студенти повинні опрацьовувати законодавчі акти, які регулюють ці питання, такі як Закон України «Про захист персональних даних» і Стратегію кібербезпеки України. У роботі необхідно подати конкретні приклади національних інформаційних ресурсів, які є місцями для забезпечення стабільності та безпеки країни, і запропонувати можливості шляхи їхнього удосконалення в умовах зростання кіберзагрози. Обсяг роботи — 7-10 сторінок.

2. Правова основа захисту персональних даних в Україні. У цьому завданні студенти повинні дослідити правові основи захисту персональних даних в Україні, звернувши увагу на відповідні законодавчі акти та нормативно-правові документи, такі як Закон України «Про захист персональних даних». Важливо відзначити, як ці акти регулюють обробку та захист персональної інформації в

державному та приватному секторах. Окремо потрібно оцінити вплив міжнародних стандартів, зокрема GDPR , на національне законодавство та практику в Україні.

8. Методи навчання

Під час викладання навчальної дисципліни використовуються методи навчання, що сприяють досягненню відповідних програмних результатів.

Результат навчання	Методи навчання
1	2
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)

9. Методи контролю

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка завдань модульного контролю, екзамен
ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка завдань модульного контролю, екзамен

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає:

– поточний, модульний та підсумковий контроль – для здобувачів денної форми навчання;

– поточний та підсумковий контроль – для здобувачів заочної форми навчання.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Модульний контроль проводиться з метою оцінювання результатів навчання здобувачів вищої освіти за модуль (змістові модулі) навчальної дисципліни. Модульний контроль проводиться під час навчального заняття після завершення вивчення матеріалу модуля (змістових модулів) навчальної дисципліни. Модульний контроль здійснюється у формі написання модульної контрольної роботи.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни або наприкінці семестру. Підсумковий контроль проводиться у формі екзамену. Процедура складання екзамену визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр
Для здобувача денної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань модульного або підсумкового контролю	40
Підсумкова семестрова оцінка	**100**
Для здобувача заочної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань підсумкового контролю	40
Підсумкова семестрова оцінка	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	48	48
Виконання та захист індивідуальних самостійних завдань	12	12
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): Підготовка наукових статей, тез доповідей наукових конференцій	до 10	до 10
Разом за виконання завдань поточного контролю	**60**	**60**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання практичних робіт	34	34
Виконання тестових завдань	14	14
Разом за виконання завдань під час навчальних занять	**48**	**48**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів під час навчальних занять може використовуватися 100-бальна шкала оцінювання щодо кожного окремо виду робіт. Розрахунок загальної кількості балів, які здобувач може набрати за результатами роботи під час навчальних занять протягом семестру, проводиться за формулою:

$$Р_{НЗ} = \sum(Р_i \times ВК_i) \times К_{НЗ}, \quad (1)$$

де $Р_{НЗ}$ – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

$Р_i$ – кількість набраних здобувачем балів за семестр за виконання і-го виду робіт під час навчальних занять (за 100-бальною шкалою);

$ВК_i$ – ваговий коефіцієнт за виконання і-го виду робіт під час навчальних занять. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, яка передбачена за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що передбачена за виконання завдань під час навчальних занять за семестр, на 100 балів.

Розподіл балів за виконання завдань модульного контролю

Види робіт здобувача вищої освіти денної форми навчання	Кількість балів за семестр
Виконання завдань модульного контролю 1	40
Разом за виконання завдань модульного контролю	**40**

Якщо здобувач вищої освіти денної форми навчання виконав завдання модульного контролю і з урахуванням отриманих балів за поточний контроль набрав у сумі 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти денної форми навчання під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі екзамену. За складання екзамену здобувач вищої освіти може набрати 40 балів. Набрані бали за виконання завдань підсумкового контролю у формі екзамену, а також бали за поточний контроль сумуються і формується семестрова оцінка з навчальної дисципліни. Бали, які здобувач вищої освіти набрав за виконання завдань модульного контролю, при цьому не враховуються під час розрахунку семестрової оцінки з навчальної дисципліни.

У здобувача вищої освіти заочної форми навчання семестрова оцінка за вивчення навчальної дисципліни формується як сума кількості балів за поточний контроль і кількості балів за підсумковий контроль.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі екзамену, якщо за виконання завдань поточного контролю набрав 20 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 15–19 балів, він отримує право за власною заявою повторно опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 14 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою повторно опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчальної дисципліни чи її окремих складових частин визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1.	Інформаційний ресурс	Information resource
2.	Доступ до інформаційних ресурсів	Access to information resources
3.	Загроза мережевій безпеці	Network security threat
4.	Атака "відмова в обслуговуванні"	Denial-of-service attack (DoS)
5.	Мережева безпека	Network security
6.	Захист мережевих пристроїв	Protection of network devices
7.	Мережева сегментація	Network segmentation
8.	Управління доступом	Access management
9.	Аутентифікація	Authentication
10.	Авторизація	Authorization
11.	Облік	Accounting
12.	Брандмауер	Firewall
13.	Технології фільтрації пакетів	Packet filtering technology
14.	Система запобігання вторгнень	Intrusion prevention system (IPS)
15.	Виявлення вторгнень	Intrusion detection
16.	Політика безпеки локальної мережі	Local area network security policy
17.	Маршрутизатор	Router
18.	Контроль доступу до мережі	Network access control
19.	Криптографія	Cryptography
20.	Алгоритм шифрування	Encryption algorithm
21.	Цифровий підпис	Digital signature
22.	Сертифікат безпеки	Security certificate
23.	Віртуальна приватна мережа	Virtual private network (VPN)
24.	Тунелювання	Tunneling
25.	Протокол безпеки	Security protocol
26.	Захист мережевого рівня	Network layer protection
27.	Захист бездротових мереж	Wireless network protection
28.	Просочування інформації	Information leakage
29.	Електромагнітне випромінювання	Electromagnetic radiation
30.	Захищені сервіси	Secured services
31.	Безпека даних у мережі	Data security in the network

12. Рекомендована література

Основна література

1. Гапак О. М., Балога С. І. Захист інформації в комп’ютерних системах. Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.

2. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навч. пос. / – Вінниця : ВНТУ, 2020. – 316 с..

3. Остапов С. Е., Євсеєв С. П., Король О.Г.. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. /– Львів: «Новий Світ- 2000», 2020 . – 678 с.

Допоміжна література

4. Хлобистова О.А. Технології захисту інформації [Електронний ресурс]:навчальний посібник / О.А. Хлобистова, Ю.Г. Савченко, М.В. Гладка – К.:НУХТ, 2014. – 84 с. Режим доступу: https://dspace.nuft.edu.ua/server/api/core/bitstreams/55a6d6da-d72b-4141-a083-6c3e90a7eccc/content
5. Тарнавський Ю. А. Технології захисту – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
6. Бобало Ю.Я. Інформаційна безпека: навч. Посібник. – Львів: Видавництво Львівської політехніки, 2019 – 580 с.
7. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

13. Інформаційні ресурси в Інтернеті

1. Закон України «Про національну безпеку України»
2. Закон України «Про основні засади забезпечення кібербезпеки України»
3. Free Software Foundation. URL: http://www.fsf.org/.
4. http://galanet.at.ua
5. http://www.osvita.info
6. https://informatic.org.ua
7. Linux in Schools project. URL: http://www.k12os.org.
8. Open Source Educational Foundation. URL: http://www.osef.org.
9. Віртуальна академія Microsoft. URL: http://www.microsoftvirtualacademy.com
10. Інтерактивне навчання за програмою Microsoft IT Academy. URL: http://itacademy.microsoftelearning.com
11. Офісний пакет LibreOffice. URL: http://www.libreoffice.org/
12. Офісний пакет WPS Office 2019. https://www.wps.com/office-free/ або http://wps-community.org/downloads
13. Офіційний сайт linuxmint. URL: http://linuxmint.com/

14. Цифрові інструменти

1. Кібергігієна для молоді. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth
2. Базові знання з кіергігієни. URL: https://osvita.diia.gov.ua/courses/basic-knowledge-of-cyber-hygiene
3. Кібергігієна: як захиститися від фішингу. URL: https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisinguttps://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu
4. Персональна кібергігієна. URL: https://osvita.diia.gov.ua/courses/personal-cyberhygiene
5. ChatGPT для підвищення власної ефективності. URL: https://osvita.diia.gov.ua/courses/chatgpt-for-personal-effectiveness

6. Датааналітик. Вступ до Excel. URL: https://osvita.diia.gov.ua/courses/data-analyst-excel

7. Демократія через дії. Модуль 1. URL: https://osvita.diia.gov.ua/courses/democracy-through-actions-module-1

8. Демократія через дії. Модуль 2. URL: https://osvita.diia.gov.ua/courses/democracy-through-actions-module-2