Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою

1. Загальна інформація

Назва дисципліни	Адміністрування в інформаційних системах
Статус дисципліни	Нормативна
Рівень вищої освіти, форма навчання	Другий (магістерський), денна форма, заочна форма
Освітньо-професійна програма	Управління інформаційною безпекою
Спеціальність	125 Кібербезпека
Рік навчання, семестр	1-й рік (1 семестр)
Мова викладання	українська
Викладач	Полотай Орест Іванович, к. т. наук, доцент кафедри управління інформаційною безпекою
E-mail	o.polotaj@ldubgd.edu.ua
Сторінка курсу в ВУ	http://virt.ldubgd.edu.ua/course/view.php?id=1550
Консультації	Згідно з розкладом консультацій кафедри управління інформаційною безпекою

2. Анотація до курсу

“Адміністрування в інформаційних системах” є дисципліною, нормативною складовою навчального плану. Дана дисципліна формує професійні компетентності здобувачів вищої освіти, які навчаються на спеціальності 125 “Кібербезпека”. Як нормативна складова, вивчення дисципліни дозволить слухачу сформувати індивідуальну освітню траєкторію.

Під час вивчення даної дисципліни слухачі отримують знання та навички, щодо адміністрування комп’ютерних мереж і систем на базі сучасного апаратного та програмного забезпечення; отримання вмінь користування практичним інструментарієм, що може бути використаний при подальшому навчанні, професійній виробничій та науковій діяльності випускника

3. Мета і завдання курсу

3.1. Метою навчальної дисципліни є надання слухачам фундаментальних теоретичних знань та формування практичних навичок з питань адміністрування інформаційних систем.

3.2. Завдання:

- формування основних знань з адміністрування інформаційних систем;
- формування та розвиток навиків самостійно розбудовувати архітектуру інформаційної системи;
- розвиток фундаментальних умінь із забезпечення адміністрування локальних мереж з метою надійного функціонування системи.

3.3. Компетентності:

Загальні компетентності:

– ЗК07 Здатність приймати обґрунтовані рішення.

Спеціальні (фахові) компетентності:

– ФК04 Здатність формулювати нові гіпотези та наукові задачі в кібербезпеці. Вибирати належні напрями і відповідні методи для розв'язання задач, беручи до уваги наявні ресурси.

– ФК05 Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.

– ФК12 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

3.4. Програмні результати навчання:

– РН04 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

– РН09 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

– РН10 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– РН12 Вирішувати задачі управління процесами відновлення функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

– РН14 Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

4. Формат і обсяг курсу

Формат курсу	Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох змістових модулів, які є логічно завершеними, відносно самостійними, цілісними частинами, засвоєння яких передбачає проведення чотирьох тестових завдань, семи лабораторних робіт та аналіз результатів їх виконання. В процесі вивчення курсу здобувачі вищої освіти також повинні брати активну участь в обговорені дискусійних питань, вирішувати індивідуально та у групі ситуативні завдання.
Обсяг дисципліни:	4 кредити / 120 академічних годин, з яких: лекцій 16 годин, лабораторних 16 годин, самостійної роботи 88 годин.
Форми навчання	лекції, лабораторні заняття, консультації, самостійна робота (в тому числі виконання здобувачами освіти індивідуальних завдань у поза аудиторний час з подальшою їх перевіркою на практичних заняттях).

5. Тематика та зміст курсу

Назви змістових модулів і тем	Кількість годин (денна форма)					Кількість годин (заочна форма)				
	усього	у тому числі				усього	у тому числі			
		л	п	лаб	с.р.		л	п	лаб	с.р.
1	2	3	4	5	6	7	8	9	10	11
Змістовний модуль 1.										
Тема 1. Створення командних файлів. Організація потоків. Сценарії входу/виходу з системи.	14	2		2	10	22	2		2	18
Тема 2. Групова політика безпеки в системі Windows. Застосовуваність групової політики безпеки. Пріорітети групової політики безпеки.	14	2		2	10	20				20
Тема 3. Поняття користувача в операційній системі. Профілі користувачів. Обмеження в профілях користувачів.	14	2		2	10	20				20
Тема 4. Поняття прав доступу. Забезпечення безпеки комп'ютерних систем з використанням політики прав доступу.	14	2		2	10	20				20
Тема 5. Використання можливостей BIOS при формуванні політики безпеки комп'ютера.	16	2		2	12	18				18
Змістовний модуль 2.										
Тема 6. Доменна модель організація мережі. Основні налаштування. Політика безпеки домену.	16	2		2	12	22	2		2	18
Тема 7. Термінальний сервер. Використання термінального сервера в віддаленому адмініструванні комп'ютерних систем.	16	2		2	12	20				20
Тема 8. Проксі-сервер як складова системного програмного забезпечення.	16	2		2	12	18				18
Усього годин	**120**	**16**		**16**	**88**	**120**	**4**		**4**	**112**

6. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1.

Тема 1. Створення командних файлів. Організація потоків. Сценарії входу/виходу з системи.
Поняття командних файлів. Потоки, процеси. Системне програмне забезпечення ОС Windows.

Тема 2. Групова політика безпеки в системі Windows. Застосовуваність групової політики безпеки. Пріорітети групової політики безпеки.
Поняття групової політики. Типи груп користувачів. Реалізація групової політики в ОС Windows.

Тема 3. Поняття користувача в операційній системі. Профілі користувачів. Обмеження в профілях користувачів.

Основні поняття профілів користувачів. Реалізація профілів користувачів в ОС Windows.

Тема 4. Поняття прав доступу. Забезпечення безпеки комп'ютерних систем з використанням політики прав доступу.

Права доступу та безпека комп'ютерних систем. Особливості політики прав доступу. Реалізація прав доступу в ОС Windows.

Тема 5. Використання можливостей BIOS при формуванні політики безпеки комп'ютера.

Загальні відомості про BIOS. Налаштування безпеки BIOS.

Змістовний модуль 2.

Тема 6. Доменна модель організація мережі. Основні налаштування. Політика безпеки домену.

Загальні відомості про домен та доменну організацію мережі. Робочі групи і домени. Доменна модель. Організація доменів і доменних імен. Простір доменних імен. Безпека в домені.

Тема 7. Термінальний сервер. Використання термінального сервера в віддаленому адмініструванні комп'ютерних систем.

Віддалене адміністрування комп'ютерних мереж. Термінальний сервер.

Тема 8. Проксі-сервер як складова системного програмного забезпечення.

Поняття проксі -серверів. Види проксі –серверів.

7. Завдання для самостійного опрацювання

З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні завдання, які отримують в кінці лабораторних занять. Практичні завдання відображені у електронному освітньому середовищі «Віртуальний університет». Перевірка правильності виконання лабораторних робіт проводиться на наступному лабораторному занятті.

8. Методи навчання

Основні форми організації навчання: лекції, лабораторні заняття із поточним контролем виконання індивідуальних завдань та проведенням тематичних тестових завдань, консультації.

Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та наочні методи навчання із елементами мозкового штурму;
- лабораторні завдання – частково-пошуковий метод навчання (певні елементи матеріалу відомі, решта студенти здобувають самостійно виконуючи завдання, розв'язуючи задачі тощо);
- консультації – словесний та дискусійний методи.

9. Технічне й програмне забезпечення /обладнання

Комп'ютери на базі процесорів Intel Pentium Gold G5400, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word, Excel, Maple), електронне освітнє середовище "Віртуальний університет"(на базі платформи Moodle).

10. Критерії оцінювання

Оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до «Положення про організацію освітнього процесу у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/polozhennya_pro_organizaciyu_osvitnogo_procesu_ldu_bzhd_nova_redakciya_10.2020.pdf та «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/polozh_ldubzhd_poryadok_ocinyuvannya_.pdf.

Поточний контроль	
Поточний контроль проводитися у формі тестування та виконання практичних завдань. Оцінювання результатів поточного контролю здійснюється за національною (чотирибальною) шкалою. Результати поточного контролю (поточна успішність) враховуються викладачем при виставленні підсумкової оцінки за диференційований залік.	
Вид робіт	**Формат проведення та критерії оцінювання**
Тестові завдання	Курсом передбачено проходження 4 тестових завдання. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 20 балів. Питання тестових завдань винесені у заліковий тест.
Робота на лабораторному занятті; самостійна робота	Курсом передбачено виконання шести лабораторних робіт. Оцінювання здійснюється за національною (чотирибальною) шкалою, відповідно до Додатку Б «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД». За роботу на практичних заняттях протягом семестру можна отримати до 30 балів.

Підсумковий контроль
Семестровий контроль проводиться у формі заліку. Допуск до семестрового контролю здійснюється за умови виконання здобувачем лабораторних робіт та успішно пройденими підсумковими тестами в середовищі «Віртуальний університет». Залік **(максимально 50 балів)** складається із двох компонентів: тестування у електронному освітньому середовищі “Віртуальний університет” та усному опитуванні.

Підсумкова семестрова оцінка обчислюється як сума балів поточного та підсумкового контролю за 100-бальною шкалою і переводяться в національну (чотирибальну) шкалу (“відмінно”, “добре”, “задовільно”, “незадовільно”, для заліків – “зараховано”, “не зараховано”).
Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості, залікової книжки (позитивні результати) здобувача в національній, 100-бальній шкалі та шкалі ЄКТС відповідно до співвідношень, поданих у наступній таблиці.

Шкала оцінювання результатів навчання здобувачів вищої освіти

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, диференційованого заліку, курсового проекту (роботи), практики	для заліку
91 – 100	**A**	відмінно	зараховано
81-90	**B**	добре	
71-80	**C**		
61-70	**D**	задовільно	
51-60	**E**		
36-50	**FX**	незадовільно	не зараховано
0-35	**F**		

11. Політика курсу

Виконання навчальних завдань і робота в курсі має відповідати вимогам «Кодекс академічної доброчесності та корпоративної культури ЛДУ БЖД»

https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/kodeks_akademichnoyi_dobrochesnosti_ta_korpo.pdf

Академічні очікування від здобувачів – своєчасне виконання завдань, передбачених силабусом дисципліни; обов'язкове відвідування і виконання практичних занять та завдань самостійної роботи.

Політика щодо термінів виконання завдань та ліквідації академічної заборгованості: терміни виконання завдань вказуються у електронному курсі «Віртуального університету». Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Відпрацювання академічної заборгованості з дисципліни можливо до дня проведення підсумкового контролю (відповідно до розкладу).
Недопущені до підсумкового контролю здобувачі освіти здійснюють перездачу в терміни, відведені для усунення академічної заборгованості у два етапи:
заборгованість із поточного контролю;
заборгованість із підсумкового контролю.
Ліквідація заборгованості поточного контролю відбувається шляхом проходження тестових завдань та виконання практичних робіт згідно із тематичним планом курсу. Ліквідація заборгованості з підсумкового контролю організовується в форматі перездачі екзамену.

Дотримання принципів академічної доброчесності: роботи (завдання) виконуються здобувачами самостійно, ідеї та ініціативи інших авторів використовуються лише при належно оформленному цитуванні.

Поведінка в аудиторії – неприпустимо запізнення та користування телефоном на заняттях, за винятком виконання громіздких обчисленнях та використанні додаткових програм в освітніх цілях; повага до думки інших колег; дотримання норм культури мовлення та ін.

12. Рекомендована література

12.1. Основна:

1. *Рамський Ю.С., Олексюк В.П., Балик А.В.* Адміністрування комп'ютерних мереж і систем: Навч. пос. — Тернопіль: Навчальна книга – Богдан, 2010. — 196 с.
2. *Клейменов С. А.* Администрирование в информационных системах : учеб. пособие для студ. высш. учеб. заведений / С. А. Клейменов, В. П. Мельников, А. М. Петраков ; под ред. В. П. Мельникова. — М.: Издательский центр «Академия», 2008. — 272 с.
3. *Поляк-Брагинский А. В.* Администрирование сети на примерах.—СПб.: БХВ-Петербург,2005. — 320 с

12.2. Додаткова:

1. *Полотай О., Бойко К.* Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78..
2. *Полотай О., Довганик С.* SIEM-системи, як елемент аналізу та управління подіями CSOC. Матер. Всеукр. наук.-практ. Internet-конф. "Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті : стан, досягнення, перспективи розвитку" (м. Черкаси, 16–22 березня 2020 р.). Черкаси : ЧНУ ім. Б. Хмельницького, 2020. С. 60–61.
3. *Полотай О., Сениш А.* Способи захисту ERP-систем. Зб. тез доп. IV Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Інформаційна безпека інформаційні технології" (м. Львів, 27 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 17–19.
4. *Polotai O., Belej O., Nestor N., Sadeckii J.* Features of Application of Data Transmission

Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.

5. *Polotai O.*, Belej O., Nestor N. Developing a local positioning algorithm based on the identification of objects in a Wi-Fi Network of the Mall. International Conference on Perspective Technologies and Methods in MEMS Designthis. 2019. Article ID 8817385. P. 32–36.
6. *Polotai O., Kukharska N., Lagun A.* The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.
7.

12.3. Інформаційні ресурси:

1. Віртуальний університет ЛДУ БЖД [Електронний ресурс]. — Режим доступу: http://virt.ldubgd.edu.ua/
2. Адміністрування інформаційних систем [Електронний ресурс] / Полотай Орест Іванович. — Режим доступу: http://virt.ldubgd.edu.ua/course/view.php?id=1550

Розглянуто на засіданні кафедри управління інформаційною безпекою
протокол від «___» _____ №___

РОЗРОБНИК
Доцент кафедри управління інформаційною безпекою, доцент

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

ЗАТВЕРДЖЕНО
Завідувач управління інформаційною безпекою
доктор тематичних наук, доцент

_____ Ростислав ТКАЧКУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Гарант освітньої програми «Управління інформаційною безпекою»
другого (магістерського) рівня вищої освіти

_____ Ростивлав ТКАЧУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту

_____ Ольга МЕНЬШИКОВА
«___» _____ 20__ р.

Дата актуалізації*					
Підпис					
Ім’я, прізвище завідувача кафедри					