Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Прус Руслана Богданівна, кандидат технічних наук
Контактна інформація	prus.ruslana@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	3 семестр, 2 курс
Обсяг дисципліни	Загальний обсяг: 135 годин, 4,5 кредити Аудиторних занять: 64, з них 30 лекції, 34 лабораторні роботи Самостійна робота: 62 години Консультації: 9 год.
Форма контролю	Екзамен
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Мова навчання	Українська
Анотація дисципліни	Дисципліна «Організаційне забезпечення захисту інформації» призначена для набуття теоретичних знань з захисту інформації та практичних навичок з організації забезпечення захисту інформації. Студенти вивчають основні напрямки, принципи та умови організаційного захисту; основні підходи, вимоги, методи та засоби, які використовують для організації системи захисту; процедуру віднесення відомостей до різних видів таємниць; порядок засекречування та розсекречування відомостей. У результаті вивчення дисципліни студенти здатні побудувати та керувати дозвільною системою доступу персоналу до конфіденційної інформації; уміють реалізовувати основні підходи та принципи організації внутрішньооб'єктового та перепусткового режимів.
Мета вивчення дисципліни	Мета навчальної дисципліни полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного управління системою захисту інформації; формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами. Основними завданнями вивчення дисципліни «Організаційне забезпечення захисту інформації» є: – розуміння вимог та задач забезпечення інформаційної безпеки; – розуміння організаційно-правового забезпечення робіт із захисту інформації; – знання нормативних документів, які регламентують діяльність в

	області захисту; – розуміння організаційно-методичних основ захисту інформації. – знання порядку віднесення відомостей до різних видів конфіденційної інформації; – знання порядку засекречування та розсекречування відомостей; – знання основних організаційних та технічних заходів з забезпечення інженерно-технічного захисту інформації.
Результати навчання	*Загальні компетентності:* 1. Здатність застосовувати знання у практичних ситуаціях. (ЗК 1). 2. Знання та розуміння предметної області та розуміння професії. (ЗК 2). 3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.. (ЗК4). 4. Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5). *Фахові компетентності:* 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. (ФК 1). 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. (ФК 2). 3. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. (ФК 5). 4. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) (ФК 7). 5. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. (ФК 8). Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки. (ФК 12). • Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібезбезпеки. *Програмні результати навчання:* Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. (ПРН 5) Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. (ПРН 8) Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. (ПРН 9) Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. (ПРН 26) Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. (ПРН 34) Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів

	системи технічного захисту інформації. (ПРН 38)
	управління доступом (мандатних, дискреційних, рольових). • Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. • Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. • Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. • Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах дотримання режиму секретності із фіксуванням результатів у відповідних документах.

Структура навчальної дисципліни

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лаб.**	**Сам. роб.**	**Конс.**	**Бали**
1	135	30	34	62	9	100
Змістовий модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації						
Тема 1. Основні положення щодо організації системи захисту інформації	8	2	2	4		2
Тема 2. Визначення інформаційних ресурсів, що підлягають захисту	9	2	2	4	1	2
Тема 3. Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту	8	2	2	4		3
Тема 4. Проведення оцінки уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз	9	2	2	4	1	3
Тема 5. Організаційна структура системи забезпечення безпеки інформації. Служба безпеки об'єкта	9	2	2	4	1	3
Тема 6. Підбір і робота з персоналом	8	2	2	4		2
Тема 7. Нормативно-правова база щодо забезпечення інформаційної безпеки	9	2	2	4	1	3
Разом за модулем 1	**60**	**14**	**14**	**28**	**4**	18

Змістовий модуль 2. Заходи з організації забезпечення захисту інформації						
Тема 8. Методи та засоби захисту інформації	8	2	2	4		3
Тема 9. Захист інформації в комп'ютерних системах від несанкціонованого доступу	9	2	2	4	1	3
Тема 10. Політика інформаційної безпеки	13	4	4	4	1	4
Тема 11. Розробка проекту системи захисту інформації	8	2	2	4		3
Тема 12. Впровадження, визначення якості і управління системою захисту інформації	9	2	2	4	1	3
Тема 13 Технології аудиту інформаційної безпеки	8	2	2	4		3
Тема 14. Структура забезпечення інформаційної безпеки	9	2	2	4	1	3
Разом за модулем 2	**64**	**16**	**16**	**28**	4	22
Модульна контрольна робота №1	4		2	2		10
Модульна контрольна робота №2	4		2	2		10
Екзамен	3			2	1	40
Разом за 3 семестр:	**135**	**30**	**34**	**62**	9	100

Оцінювання

При вивченні дисципліни студент виконує такі види робіт: опрацювання теоретичного матеріалу та виконання лабораторних робіт, виконання індивідуальних завдань, написання тестів.

Рівень знань студента оцінюється в балах, фіксується в журналі після вивчення змістового модуля. Підсумкова оцінка за національною шкалою за семестр заноситься в заліково-екзаменаційну відомість.

Усі види навчальної діяльності студента оцінюються певною кількістю балів. Підсумковий контроль здійснюється у формі екзамену. Сумарна кількість балів, яку студент отримує при засвоєнні змістових модулів за 100-бальною шкалою, визначає його підсумкову оцінку.

Дисципліна складається з двох змістових модулів. Підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

1. поточне оцінювання (максимум 40 балів);
2. екзамен (максимум 60 балів).

Поточний контроль, який має на меті перевірку рівня знань студента, здійснюється викладачем упродовж семестру у межах змістових модулів. Поточний контроль включає оцінку поточної роботи студента у ході виконання лабораторних робіт. Максимальна кількість балів за результатами поточного контролю становить 40 балів.

Підсумковий контроль, який здійснюється викладачем, має на меті перевірку рівня знань студента під час виконання екзаменаційного тесту, виконання практичного завдання та усної

відповіді. Максимальна кількість балів, яку студент може набрати за екзамен, становить 60 балів, з яких по 10 балів – це оцінка за кожну із двох модульних контрольних робіт.

Поточний контроль (мах = 40 балів)		**Модульний контроль/екзамен (мах = 60 балів)**			**Загальна кількість балів**
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	**Екзамен**	
20	20	10	10	40	100

Підсумковий контроль

Екзамен складається з трьох частин: 1) написання екзаменаційного тесту (максимум – 20 балів); 2) виконання практичного завдання (максимум 10 балів) та 3) усна відповідь (максимум – 10 балів).

В оцінці знань студентів враховується:

1) достатність обсягу відповіді (повна, недостатньо повна, неповна);

2) обізнаність з основними поняттями, принципами, законами, правилами навчальної дисципліни;

3) логічність викладу матеріалу;

4) обґрунтованість власних міркувань;

5) уміння інтегрувати та диференціювати знання теоретичного матеріалу та застосовувати їх при виконанні практичних завдань.

Відповідь вважається *повною* (*40 балів*), якщо студент повністю оволодів матеріалом, обізнаний з усіма поняттями і термінами навчального курсу і адекватно оперує ними під час відповідей на поставлені питання, а також посилається на наукові дослідження з навчальної дисципліни, ознайомлений зі спеціальною літературою; демонструє здатність аналізувати факти, аргументувати власні судження теоретичними і фактичними положеннями, підсумувати сказане висновками.

Відповідь вважається *недостатньо повною* (*36 балів*) за умов непоганого володіння знаннями з навчального предмету. Відповідь студента має бути правильною й обгрунтованою. Студент повинен продемонструвати знання теоретичного матеріалу, навички самостійної навчально-пізнавальної діяльності, здатність викладати матеріал в певній логічній послідовності. Допускаються незначні помилки, які не впливають на загальне розуміння викладеного матеріалу.

Відповідь вважається *неповною* (*32 бали*), якщо продемонстровані знання з предмету носять фрагментарний і поверхневий характер. Теоретичні і фактичні знання відтворюються репродуктивно, без глибокого осмислення, аналізу, порівняння, узагальнення. Студент обізнаний з літературними джерелами з навчальної дисципліни, але не може дати достатньо критичної їх оцінки; допускає суттєві помилки, які порушують логіку викладення матеріалу.

Екзамен вважається *нескладеним (нижче 24 балів),* за умов неправильної або неповної відповіді, яка свідчить про нерозуміння поставленого завдання. Студент не володіє понятійно-категоріальним апаратом, необізнаний з джерельною базою з навчальної дисципліни і допускає грубі помилки у викладенні матеріалу.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури;

підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування.

Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна у встановлені викладачем терміни під час консультацій.

Перескладання модулів відбувається із дозволу викладача за наявності поважних причин (наприклад, лікарняний).

Рекомендована література та інтернет-ресурси

1. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. No 423.
2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. No 511.
3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. No 200.
4. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2000. [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_1023_75718671.pdf]
5. НД ТЗІ 2.7-011-2012 "Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв". – 2012 [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_5623_75714589.pdf].
6. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю / 27 березня 2019 р. за N 306/33277 [Електронний ресурс]. – Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].
7. Постанова Кабінету Міністрів України від 29.03.2006 No 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. –Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].
8. Захист інформації в автоматизованих системах управління : навчальний посібник /

Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

9. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

10. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К.: ДУТ- КНУ, 2016. – 178 с.

11. Логінова Н. І. Правовий захист інформації: навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

12. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.

13. Носов В.В., Манжай О.В. Організація та забезпечення інформаційної безпеки: Навч. посібник. – Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2007.

14. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

15. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця: ВНТУ, 2017. – 120 с.

Силабус навчальної дисципліни, затверджено на засіданні кафедри

Комп'ютерних наук та кібербезпеки
протокол № 3 від 05.10.2020р.

Завідувач кафедри:  Сачук Ю.В.