НАВЧАЛЬНИЙ КУРС (*Syllabus* = ОП + НП + РНПД + розклад + Ви кладач)		
Група полів	*Поле*	
Назва	– код у загальноуніверситетському класифікаторі (шифр спец. + рівень освіти{Б/М/А/Д} + шифр дисц. за ОП) + назва за ОП {посилання на місце у *Навчальному Плані*}	**029БВБ20.1 Захист інформації**
Анотація курсу	– перелік тем [питань], що розглядаються у дисципліни	**Змістовий модуль 1. Поняття інформаційної безпеки та її місце в системі національної безпеки.** **Тема 1.** Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ**.** Види інформації. Основні поняття захисту інформації(об'єкти, суб'єкти, канали витоку, НСД, рівні доступу). Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ. Поняття політики забезпечення ІБ. Структура, задачі служби Інформаційної безпеки. **Тема 2.** Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки.. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки. **Тема 3.**. Внутрішні механізми розмежування доступу (маркери доступу і дескриптори захисту), структура і призначення, участь маркерів доступу і дескрипторів захисту в процедурі одержання суб'єктів

		доступу до об'єктів ОС Механізми аудита і протоколювання в ОС Windows, класи зареєстрованих подій, керування аудитом (включення, відключення аудита визначених подій), аудит доступу до об'єктів і реєстру, журнали аудита, правила звертання з журналами аудита. Права ФС NTFS, призначення прав, керування правами, визначення діючих прав, перевірка прав при звертанні до об'єкта ФС. **Змістовий модуль 2. Організація захисту інформації** . **Тема 4.** Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Особливості організації захисту від різних видів шкідливого програмно забезпечення.. Файлово-серверна і клієнт-серверна архітектури: опис, переваги і недоліки системи з колективним використанням файлів,системи з архітектурою клієнт-сервер: організація, достоїнства і недоліки. **Тема 5**. Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Класична шифри. Криптографічні і стеганографічні методи захисту інформації. **Тема 6**. Симетричні шифри. Види симетричних шифрів. Математичні алгоритми. Стандарти симетричних шифрів Лабораторне заняття №8 (4 години) **Тема 7.**Асиметричні шифри. Математичні алгоритми. Стандарти асиметричних шифрів. Криптологічні протоколи
	– перелік дисциплін, які є передумовою вивчення курсу	«Документно-інформаційні комунікації»
	– перелік дисциплін, для яких курс є передумовою	«Виконання кваліфікаційної роботи»
	– очікуваний результат	Результати навчання з дисципліни відповідно до освітньо-професійної програми (та програмних результатів навчання) виявляються в тому, що студенти повинні **знати:**

		• канали уразливості та витоку інформації, явища, що притаманні їх прояву та існуванню; • основні методи, механізми, протоколи та алгоритми криптографічного захисту інформації; • критерії та показники оцінки якості криптографічного захисту інформації; • методи криптографічних перетворень інформації та способи їх здійснення; • методи та засоби аналізу та крипто аналізу асиметричних та симетричних крипто перетворень; • основні протиріччя, проблеми, тенденції та напрями розвитку теорії та практики криптографічного захисту інформації, прогнозування їх можливостей та можливостей порушників(крипто аналітиків); • функціональні можливості та порядок застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек. **а також уміти:** • розробляти політику безпеки згідно світовим стандартам, проводити аналіз погроз безпеці інформації та володіти основними методами, механізмами, алгоритмами захисту інформації в інформаційно – комунікаційних системах з урахуванням сучасного стану та прогнозу здійснення погроз • обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів; • розробляти вимоги та обирати для застосування криптографічні перетворення та протоколи, що мінімізують впливи порушників; • розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу криптографічних алгоритмів та протоколів захисту

		інформації..
Місце курсу у НП	– [розподіл по семестрах]	Четвертий рік, осінній семестр
	– обсяг кредитів	Осінь – 4 кредити.
	– тижневе навантаження (лекції + практична частина)	(2 – 2).
	– форма контролю	Залік.
Зміст курсу	– лекційний курс (тема розділу + питання для самост. роботи ***виділені жирним курсивом***)	**Змістовий модуль 1. Поняття інформаційної безпеки та її місце в системі національної безпеки.** **Тема 1.** Види і джерела погроз ІБ. Система нормативно-правових актів, що регламентують забезпечення ІБ**.** Види інформації. Основні поняття захисту інформації(об'єкти, суб'єкти, канали витоку, НСД, рівні доступу). Протиправна діяльність в інформаційній сфері. Карно-процесуальна характеристика комп'ютерних злочинів. Основні задачі організаційної системи забезпечення ІБ. Поняття політики забезпечення ІБ. Структура, задачі служби Інформаційної безпеки. ***1. Протиправна діяльність в інформаційній сфері.*** ***2. Карно-процесуальна характеристика комп'ютерних злочинів.*** **Тема 2.** Модель Белла-Лападули, як основа побудови систем мандатного розмежування доступу. Основні положення моделі. Основна теорема безпеки.. Види і джерела погроз ІБ: а) дискреційна політика безпеки; б) мандатна політика безпеки. ***1. Збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС*** **Тема 3.**. Внутрішні механізми розмежування доступу (маркери доступу і дескриптори захисту), структура і призначення, участь маркерів доступу і дескрипторів захисту в процедурі одержання суб'єктів доступу до об'єктів ОС Механізми аудита і протоколювання в ОС Windows, класи зареєстрованих подій, керування аудитом (включення,

		відключення аудита визначених подій), аудит доступу до об'єктів і реєстру, журнали аудита, правила звертання з журналами аудита. Права ФС NTFS, призначення прав, керування правами, визначення діючих прав, перевірка прав при звертанні до об'єкта ФС. ***1. Облікові записи користувачів і груп, збереження інформації про облікові записи на твердому диску, класична атака по скиданню і підборові пароля користувача, способи захисту система, реалізація,методи збереження інформації про дискові блоки, що належать файлові в FAT, Ext2, NTFS, засобу забезпечення надійності і високої продуктивності ФС.*** **Змістовий модуль 2. Організація захисту інформації** . **Тема 4.** Бази даних, класифікація баз даних, поняття цілісності і несуперечності бази даних, методи і засоби забезпечення цілісності і несуперечності. Особливості організації захисту від різних видів шкідливого програмно забезпечення.. Файлово-серверна і клієнт-серверна архітектури: опис, переваги і недоліки системи з колективним використанням файлів,системи з архітектурою клієнт-сервер: організація, достоїнства і недоліки. ***1. Основні історичні етапи становлення криптографії.*** **Тема 5**. Основні поняття криптографії. Стійкість шифрів. Теоретична і практична стійкість криптосистем. Узагальнена схема для криптосистем із закритими ключами шифрування. Класична шифри. Криптографічні і стеганографічні методи захисту інформації. **Тема 6**. Симетричні шифри. Види симетричних шифрів. Математичні алгоритми. Стандарти симетричних шифрів ***1. Криптографічні і стеганографічні методи захисту інформації*** **Тема 7.**Асиметричні шифри. Математичні алгоритми. Стандарти асиметричних шифрів. Криптологічні протоколи ***1. Основні задачі організаційної системи забезпечення ІБ.*** ***2. Поняття політики забезпечення ІБ***

	– навчальна література	**Базова** 1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р. 2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р. 3. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с. 4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с. 5. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с. 6. Головко Г.В**.** Лабораторний практикум З дисципліни «захист інформації» Для Спеціальності - « інформаційна, бібліотечна та архівна справа» Для студентів всіх форм навчання Полтавський національний технічний університет імені Юрія Кондратюка. – Полтава, 2018. – 59с. **Допоміжна** 1. Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с. 2. Бембо Мао. Современная криптографія. Теорія и практика. Москва. 2005. 3. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с. 4. Б. Шнайер . Безопасность данных в цифровом мире. Изд. Питер. Харьков. 2003 г. 367 с. 5. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”. К. 2001. 669 с. 6. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Також «Введение в криптографию» под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html). 7. А. Менезис, П. Ван Аршот, С. Ватсон. Руководство по прикладной

		криптографии CRC Press, 1997, электронная копия, 662 с. 8. Бессалов А., Телиженко А. Криптосистемы на эллиптических кривых. – К.: «Політехніка», 2004. – 224 с. 9. Радіотехніка № 114, 119, 126, 134, 141, 142,145.Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000- 2008 рр. 10. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» №2- 2006; №2, №3-2007, №3- 2008, №3 – 2009, № 3 – 2010, №2 – 2011рр. **Інформаційні ресурси** 1. Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України". 2. Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР. 3. Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР. 4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV. 5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX. 6. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
Координатори курсу	– ім'я + прізвище координатор {посилання на *Profile*}	Геннадій Головко, к.т.н., доцент.
	– ім'я + прізвище асистента координатора {посилання на *Profile*}	-
Розклад	– період вивчення (дата початку – дата завершення)	Вересень – грудень 2020 р.

	– тривалість (кількість тижнів)	
	– тривалість (хв.)	80 хв.
	– аудиторія	Згідно з розкладом
Політика курсу	{посилання на загальні правила допуску та вивчення навчальних курсів на сторінці університету/інституту/факультету} (критерії оцінювання + складові підсумкової оцінки + тощо)	Загальна трудомісткість дисципліни – 100 балів, із них: при підсумковому контролі у вигляді заліку до 70 балів студент може отримати впродовж семестру, решта 30 балів припадає на підсумковий контроль; **1. Поточний контроль.** Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином (розподіл орієнтовний): - робота на семінарських заняттях (відповіді на практичних заняттях, виконання практичних завдань, розв'язання тестових питань на платформі дистанційного навчання Moodle), у разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять) – до 50 балів. Присутність на лекціях і практичних заняттях не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів, при тривалій відсутності студента на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії. Студент, який повністю виконав програму навчальної дисципліни й отримав достатню рейтингову оцінку (не менше 35 балів), допускається до підсумкового контролю з дисципліни. **2. Підсумковий контроль** Підсумковим контролем є залік. Він здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті «Полтавська політехніка імені Юрія Кондратюка» (https://nupp.edu.ua/uploads/files/0/doc/polozhennia/organizacia-osvit-procesu.pdf), а також «Положення про семестровий контроль в Національному університеті «Полтавська політехніка імені Юрія Кондратюка» (https://nupp.edu.ua/uploads/files/0/doc/polozhennia/semestr-kontrol.pdf.) Залік проводиться у тестовій формі.

Рекомендації до вивчення курсу	Загальні настанови та рекомендації щодо вивчення навчального курсу та підготовки до контрольних заходів	Для належного опанування дисципліною слід опрацювати базову літературу, засвоїти відповідну нормативно-правову базу, засвоїти термінологію. Особливо ретельно слід зосередитись на набутті практичних навичок з навчальної дисципліни.
Примітки		

Примітки: 1. **РНПД** – робоча навчальна програма дисципліни.
2. **ОП** – освітня програма.
3. **НП** – навчальний план.