ІНФОРМАЦІЯ ПРО ДИСЦИПЛІНИ ВІЛЬНОГО ВИБОРУ
Спеціальність 125 Кібербезпека
Освітньо-наукова програма "Інформаційна безпека держави"

Назва дисципліни (кількість кредитів, семестр) ПІП викладача	Анотація	Форма підсумкового контролю
Системний аналіз та прийняття рішень в інформаційній кібербезпеці (4 кредити, 1 – 2 семестри)	Дисципліна «Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» передбачає вивчення основних понять, структури, основних завдань та методів системного аналізу і теорії прийняття рішень; технологій застосування системного аналізу та прийняття рішень в інформаційній безпеці; формування умінь та навичок із системного аналізу та системного підходу при прийнятті рішень достатніх для застосування і подальшого продовження самоосвіти у галузі інформаційної безпеки та захисту інформації; отримання кваліфікації аналітика даних, спеціаліста аналізу даних, бізнес-аналітика ІКТ, Web-аналітика тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 р.). **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно досліджувати пізнавальну та реалізовувати прогнозуючу функції щодо теорії і практики прийняття рішень та оцінювання отриманих результатів. *Пізнавальна функція* проявляється в розкритті сутності процесів прийняття рішень, закономірностей і принципів, яким вона підкоряється, поясненні основних властивостей і взаємозв'язків предмета дослідження, обґрунтуванні технології та системи прийняття рішення. *Прогнозуюча* полягає у визначенні тенденцій подальшого розвитку процесів і системи прийняття рішення, організаційних форм і методів діяльності персоналу управління в процесі прийняття рішення. **Поняттєве поле:** системний підхід, системний аналіз, категорії системного підходу, система, класифікація систем, структура системи, організація системи, цілі системи, система захисту інформації, системний підхід до захисту інформації, системне проектування систем захисту інформації, класифікація моделей, системні принципи моделювання, інформаційна система, система захисту інформації в інформаційній системі, моделювання об'єктів захисту, автоматизована система обробки даних, рішення, теорія прийняття рішень, задача прийняття рішень, системний підхід до процесу прийняття рішень рішення, прийняття рішень в умовах визначеності, прийняття рішень в умовах ризику та невизначеності, теорія ігор, прийняття рішень в умовах конфлікту, експертиза, експертне оцінювання, аналіз матеріалів експертного оцінювання, Парето-аналіз, критерії оцінювання систем безпеки, проблема вибору раціонального варіанта системи захисту інформації.	**Залік**

Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності (4 кредити, 1 – 2 семестри)	Дисципліна «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно формувати обґрунтовані судження про можливий стан систем захисту та/або систем інформаційної і кібербезпеки в майбутньому та (або) про альтернативні шляхи і терміни їх реалізації. Головними функціями прогнозування перспектив розвитку систем захисту при цьому є: науковий аналіз процесів і тенденцій; дослідження об'єктивних зв'язків явищ в розвитку; оцінка об'єкта прогнозування (базується на поєднанні аспектів детермінованості (обмеження) і невизначеності; виявлення альтернатив розвитку; накопичення наукового матеріалу для обґрунтування вибору управлінських рішень. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно формувати обґрунтовані судження про можливий стан систем захисту та/або систем інформаційної і кібербезпеки в майбутньому та (або) про альтернативні шляхи і терміни їх реалізації. Головними функціями прогнозування перспектив розвитку систем захисту при цьому є: науковий аналіз процесів і тенденцій; дослідження об'єктивних зв'язків явищ в розвитку; оцінка об'єкта прогнозування (базується на поєднанні аспектів детермінованості (обмеження) і невизначеності; виявлення альтернатив розвитку; накопичення наукового матеріалу для обґрунтування вибору управлінських рішень. **Поняттєве поле:** прогнозування, типологія прогнозів, цільове угруповання прогнозів, прогнозне поле, способи та методи науково-технічного прогнозування, схема прогнозування, модель прогнозу, експертні оцінки, типи моделювання, класифікація моделей, їх властивості, види та етапи моделювання, структури систем, дослідження моделей систем.	**Залік**
Проєктування і впровадження захищених інформаційно-комунікаційних систем (4 кредити, 5 семестр)	Дисципліна «Проєктування і впровадження захищених інформаційно-комунікаційних систем» передбачає вивчення технологій розробки захищених інформаційно-комунікаційних систем, а також проєктування відповідних комплексів засобів захисту інформації в ІКС; формування: умінь та навичок з розроблення систем захисту ІКС й визначення загальних принципів їх побудови; формування опису ІКС та середовища їх функціонування; визначення складу апаратного та програмного забезпечення; здійснення аналізу обчислювальних процесів та технологій; формування політик і правил забезпечення безпеки тощо; отримання: кваліфікації фахівця з питань обслуговування мереж, фахівця з ІКТ безпеки, консультанта з питань ІКТ безпеки, тестувальника систем безпеки, експерта з кібернетики, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року). **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор	**Залік**

	філософії» професійних компетенцій щодо проектування КЗЗ інформації та здатностей самостійно створювати захищені ТСМ. Завданнями дисципліни є формування умінь із: розробки загальних підходів до проектування захищеної ТСМ; застосування національних і міжнародних стандартів при розробці вимог до захищеної ТСМ; розробки політик безпеки для ТСМ; проектування окремих засобів захисту та їх інтеграції до комплексу засобів захисту ТСМ; створення перспективних КЗЗ ТСМ. **Поняттєве поле:** захищені ІТ системи, методологія та методи проектування систем захисту, проектування захищених інформаційних систем, аналіз захищеності, технологічна модель, технологічна модель інформаційної безпеки, концепція захищених мереж, забезпечення інформаційної безпеки, інструменти забезпечення безпеки інформації, алгоритми, моделі, методи, програмні комплекси кібербезпеки, адміністрування, експлуатація, адміністрування захищених систем, експлуатація захищених систем, права доступу, правила забезпечення безпеки, цілісність даних, теорія ігор, марківські процеси, мережа Петрі, нечіткі множини.	
Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем (4 кредити, 5 семестр)	Дисципліна «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно оволодіти студентами сучасними технологіями адміністрування та захисту інформації в інформаційно-комунікаційних системах та мережах, особливостями їх реалізацій, принципами побудови та адміністрування програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах та мережах. Завдання дисципліни полягає у набутті студентами знань, умінь і здатностей (компетенцій) адміністрування в інформаційно-комунікаційних системах та мережах для ефективного вирішення завдань професійної діяльності. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно оволодіти сучасними технологіями адміністрування та захисту інформації в інформаційно-комунікаційних системах та мережах, особливостями їх реалізацій, принципами побудови та адміністрування програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах та мережах. Завдання дисципліни полягає у набутті здобувачами знань, умінь і здатностей (компетенцій) адміністрування в інформаційно-комунікаційних системах та мережах для ефективного вирішення завдань професійної діяльності. **Поняттєве поле:** середовище експлуатації, загрози безпеці інформації в захищених інформаційно-комунікаційних системах (ЗІКС), політики безпеки в ЗІКС, керування	**Залік**

	доступом до інформації у ЗІКС, системи антивірусного захисту, політики облікових записів в операційних системах, організація безпеки даних, безпеки локальних мереж, безпеки механізмів аутентифікації, організація шифрування трафіку.	
Організація захисту розподілених інформаційних ресурсів (4 кредити, 5 – 6 семестри)	Дисципліна «Організація захисту розподілених інформаційних ресурсів» передбачає вивчення технологій створення і принципів роботи розподілених файлових систем; технологій проєктування систем захисту інформації в розподілених ІС (РІС); технологій оптимізації та пошуку і прийняття рішень при створенні систем захисту РІС; Технології обміну інформацією в РІС; формування умінь та навичок з вибору засобів ОС та програмно-апаратного забезпечення для розробки розподілених додатків; проєктування і розробки РІС та систем їх захисту; підтримки працездатності РІС в заданих функціональних характеристиках та забезпечення їх відповідності заданим критеріям якості, тощо; отримання кваліфікації фахівця з питань обслуговування мереж, розробника та інтегратора БД; адміністратора мережі ІКТ; директора з ІКТ безпеки; адміністратора Web-сайту; менеджера з розвитку Web-бізнесу; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року). **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно досліджувати особливості захисту інформаційних ресурсів у розподілених інформаційних системах (РІС). Опанування навчальним матеріалом дозволить критично обирати ті механізми підвищення живучості РІС, які є найбільш ефективними в кожному конкретному випадку та застосовувати їх при побудові сучасних систем захисту. **Поняттєве поле:** розподілені системи, вразливості, загрози, безпека даних, протокол P2P, атака, напад, координація систем, групове спілкування, пом’якшення атак, ресурс, координація системи, інформаційна інфраструктура.	**Залік**
Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем (4 кредити, 5 – 6 семестри)	Дисципліна «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення системи моніторингу та аудиту стану інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах. Завданнями навчальної дисципліни є формування умінь із: обґрунтування варіантів побудови автоматизованої системи моніторингу та аудиту стану інформаційної безпеки для розподіленої обчислювальної системи та її основні складові: систему аналізу вразливостей, систему виявлення вторгнень, систему управління комплексною системою захисту інформації; застосування міждержавних та вітчизняних стандартів при створенні системи моніторингу та аудиту стану ІБ; створення перспективних систем моніторингу та аудиту стану ІБ. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення системи моніторингу	**Залік**

	та аудиту стану інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах. Завданнями навчальної дисципліни є формування умінь із: обґрунтування варіантів побудови автоматизованої системи моніторингу та аудиту стану інформаційної безпеки для розподіленої обчислювальної системи та її основні складові: систему аналізу вразливостей, систему виявлення вторгнень, систему управління комплексною системою захисту інформації; застосування міждержавних та вітчизняних стандартів при створенні системи моніторингу та аудиту стану ІБ; створення перспективних систем моніторингу та аудиту стану ІБ. **Поняттєве поле:** властивості процесів і систем, методи оцінки інформаційної безпеки, системи моніторингу, аудит автоматизованих інформаційних систем, ідентифікація ,вразливостей ліквідація вразливостей, оцінка захищеності інформації від несанкціонованого доступу, системи керування мережею, системи діагностики та управління, експертні системи, активний моніторинг, пасивний моніторинг, аналізатори протоколів.	
Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів (3 кредити, 6 семестр)	Дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» передбачає вивчення способів формування вимог до систем безпеки об'єктів критичної інфраструктури (ОКІ); положення стандартів та нормативно-правових документів забезпечення їх захисту АСУ ОКІ від стороннього кібернетичного впливу; формування умінь та навичок з вибору стратегії дій на основі системного підходу використовуючи оброблену отриману інформацію; розробки неформалізованих моделей засобів, систем і процесів, що застосовуються в ОКІ та їх аналізу з точки зору ІКБ; забезпечення функціонування ОКІ в частині виконання вимог ІКБ; розробки планів і проведення заходів щодо організації захисту інформації (забезпечення кібербезпеки) ОКІ; побудови та перевірки моделей аналізу і синтезу інформаційно-комунікаційних систем та мереж; отримання кваліфікації аналітика даних, Web-аналітика, ризик-менеджера, менеджера соціальних мереж, консультанта з питань ІКТ безпеки, експерта з кібернетики, директора з ІКТ безпеки; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року). **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно створювати та аналізувати різноманітні типові технології побудови систем інформаційної та кібернетичної безпеки сучасного підприємства, проектувати та впроваджувати базові варіанти побудови системи ІКБ, тощо. Завданнями дисципліни є формування умінь із: створення безпечних інформаційних систем та підтвердження їх відповідності; застосування сучасних технологій створення та експлуатації систем інформаційної та	**Залік**

	кібернетичної безпеки сучасного підприємства забезпечення інформаційної та кібернетичної безпеки сучасного підприємства. **Поняттєве поле:** захищені об'єкти інформаційної діяльності (ОІД), методологія захисту інформації на ОІД, методи захисту інформації на ОІД, проектування систем захисту, проектування захищених інформаційних систем, аналіз захищеності ОІД, технологічна модель захисту ОІД, концепція захисту інформації на ОІД, інструменти забезпечення безпеки інформації, концепція захисту інформації, технологічна модель, алгоритми захисту, моделі захисту, методи захисту, програмні комплекси кібербезпеки ОІД, об'єкт критичної інфраструктури, ведення кібердій і кіберконфліктів, адміністрування, експлуатація, адміністрування захищених систем, експлуатація захищених систем, права доступу, правила забезпечення безпеки, цілісність даних.	
Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури (3 кредити, 6 семестр)	Дисципліна «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та ІТС, здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації. Завданнями дисципліни є формування умінь із побудови систем захисту інформації адміністрування систем захисту інформації. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та ІТС, здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації. Завданнями дисципліни є формування умінь із: побудови систем захисту інформації; адміністрування систем захисту інформації. **Поняттєве поле:** критичні процеси об'єкта критичної інфраструктури, інформаційні ресурси, управління доступом, мережевий захист інформаційних ресурсів об'єкта критичної інформаційної інфраструктури, політика управління ризиками інформаційної безпеки, методика оцінювання ризиків інформаційної безпеки, політика управління обліковими записами, політика мережевого захисту.	**Залік**
Технології безпеки складних соціотехнічних систем (3 кредити, 3 семестр)	Дисципліна «Технології безпеки складних соціотехнічних систем» передбачає вивчення сучасного стану проблеми безпеки в соціотехнічних системах (СТС), що є складною сукупністю взаємодій людини, інформаційної системи, навколишнього середовища в	**Залік**

	умовах впливу на них соціальних, економічних, політичних, природних, технічних та інших факторів; формування умінь та навичок з проведення оцінку безпеки СТС по заданому критерію; прогнозування можливих витоків повідомлень в СТС, моделювання систем захисту; імовірнісного аналізу помилок в повідомленні та сумарних помилок на різних рівнях інформаційного взаємодії; отримання кваліфікації аналітика клієнтського досвіду, менеджера з оптимізації пошукових систем, Web-розробника, ризик-менеджера, менеджера соціальних мереж, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера IT та цифрові професії» від 03.09.2020 року). **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей виявлення інформаційно-кібернетичних та інформаційно-психологічних атак на соціотехнічні системи, а також розробки та впровадження низки заходів захисту, необхідних для попередження таких атак. Завданнями дисципліни є формування умінь із: виявлення інформаційно-кібернетичних та інформаційно-психологічних атак в різних умовах функціонування соціотехнічних та комп'ютерних систем; оцінювання підготовленості персоналу у сфері соціотехнічної безпеки та їх можливостей із побудови та підтримки працездатності систем захисту від інформаційно-кібернетичних та інформаційно-психологічних атак. **Поняттєве поле:** інформаційні відносини, інформаційна війна, порушення, інформаційне протиборство, управління комплексною інформаційною безпекою, оцінювання інформаційної стійкості, логіко-ймовірнісна модель, соціотехнічні атаки, методи соціального інжинірингу, маніпулювання, когнітивні упередження, соціальна інженерія, атака, фішинг, точка доступу, захист персональних даних, реверсивна соціальна інженерія, порушник, атака, експертна оцінка, оцінювання захищеності інформації, персонал, соціоінженерний підхід, ризик, оцінка ризику.	

Прикладні аспекти протидії кібератакам в соціотехнічних системах (3 кредити, 3 семестр)	Дисципліна «Прикладні аспекти протидії кібератакам в соціотехнічних системах» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійної реалізації інформаційних операцій і атак в соціотехнічних системах, розробки організаційно-правових заходів захисту, необхідних для попередження атак в сфері управління ІБ. Завданнями дисципліни є формування умінь із реалізації інформаційних операцій і атак на соціотехнічні системи застосування механізмів оцінки та побудови заходів захисту від інформаційних операцій і атак в сфері управління інформаційною безпекою. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійної реалізації інформаційних операцій і атак в соціотехнічних системах, розробки організаційно-правових заходів захисту, необхідних для попередження атак в сфері управління ІБ. Завданнями дисципліни є формування умінь із: реалізації інформаційних операцій і атак на соціотехнічні системи; застосування механізмів оцінки та побудови заходів захисту від інформаційних операцій і атак в сфері управління інформаційною безпекою. **Поняттєве поле:** соціотехнічні атаки, соціальна інженерія, загрози соціального інжинірингу, реверсивна соціальна інженерія, особистісні підходи, методи та засоби протидії соціотехнічним атакам, експертне оцінювання.	**Залік**
Прикладні аспекти математичних методів у системах виявлення та попередження кіберзагроз (4 кредити, 1 – 2 семестри)	Дисципліна «Прикладні аспекти математичних методів у системах виявлення та попередження кіберзагроз» передбачає вивчення математичних методів, які знайшли застосування в задачах побудови ефективних систем виявлення та попередження вторгнень у кіберпросторі. Завдання дисципліни полягає у набутті знань, умінь та навичок щодо використання статистичних методів, зокрема, методів кластерного аналізу, методу опорних векторів та методу непараметричної регресії; методів природних обчислень (штучні нейронні мережі, штучні імунні мережі); методів, які ґрунтуються на правилах нечіткої логіки, та математичного апарату теорії ігор як для виявлення зловживань, так і для виявлення мережевих аномалій. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій щодо використання математичних методів у системах виявлення та попередження кіберзагроз, а також здатностей самостійно проводити порівняльний аналіз розглянутих методів з метою розробки удосконалених комбінацій, які будуть відрізняться низькою обчислювальною складністю, високою адаптивністю, достатньою стійкістю, мінімальною кількістю хибних спрацьовувань, коректністю, верифікованістю та ін. **Поняттєве поле:** системи виявлення та попередження вторгнень; математичні моделі; статистичні методи, приховані марковські моделі, метод опорних векторів, кластерний аналіз, штучні нейронні мережі, штучні імунні мережі, нечітка логіка, теорія ігор,	**Залік**

	прийняття рішень в умовах конфлікту, оптимальні стратегії.	
Прикладний функціональний аналіз (4 кредити, 5 семестр)	«Функціональний аналіз» - розділ сучасної математики, що досліджує нескінченновимірні простори та їх відображення і є узагальненням та синтезом ідей і методів класичного математичного аналізу, теорії диференціальних рівнянь, лінійної алгебри, геометрії та, завдяки своїй абстрактності, має широке прикладне застосування як в самій математиці, так і в дотичних до неї галузях. Навчальна дисципліна «Прикладний функціональний аналіз» передбачає ознайомлення здобувачів освіти з основними принципами лінійного функціонального аналізу в нормованих просторах, теорією гільбертових просторів і ортогональних базисів, основами теорії міри та інтеграла Лебеґа, необхідними для дослідницької або інноваційної роботи у сфері практичних застосувань зазначених теорій. **Мета курсу**: дати студентам основи знань з теорії міри, вимірних функцій та інтеграла Лебеґа, теорії метричних просторів, лінійних нормованих просторів та лінійних обмежених операторів, розглянути деякі їх прикладні застосування. **Поняттєве поле**: збіжність в метричних просторах, компактність множин, принцип стискуючих відображень, лінійні нормовані простори, збіжність в лінійних нормованих просторах, банахові та гільбертові простори, лінійні неперервні оператори і функціонали, узагальнені функції, прикладні застосування функціонального аналізу.	**Залік**
Математичне моделювання в криптографії на основі діофантових рівнянь (3 кредити, 6 семестр)	Навчальна дисципліна «Математичне моделювання в криптографії на основі діофантових рівнянь» передбачає ознайомлення здобувачів із одним із сучасних методів математичного моделювання в розробці систем захисту інформації з використанням алгебраїчних діофантових рівнянь. Такі методи спрямовані на створення таких систем захисту, які унеможливлюють нелегальному користувачу можливість скоротити множину ключів. **Мета курсу**: дати студентам основи знань з теорії діофантових рівнянь, ознайомити з розв’язанням 10-ї проблеми Гільберта, продемонструвати можливість використання багатостепеневих систем діофантових рівнянь для розробки стійких до зламу систем захисту інформації, ознайомити з найновішими результатами в цьому напрямі. **Поняттєве поле**: Діофантові рівняння, 10-а проблема Гільберта, задачі з «діофантовими труднощами», багатостепенева система діофантових рівнянь, параметричний розв’язок, симетрична криптосистема, дисиметрична криптосистема.	**Залік**

Методи математичної статистики в наукових дослідженнях (4 кредити, 5-6 семестр)	Програма визначає обсяги знань, якими повинен опанувати здобувач вищої освіти ступеня доктора філософії (далі - здобувач) відповідно до національної рамки кваліфікації, алгоритму вивчення навчального матеріалу дисципліни вибіркової частини «Методи математичної статистики в наукових дослідженнях» та необхідне методичне забезпечення, складові і технологію здійснювання статистичного аналізу отриманих даних. Навчальна дисципліна “ Методи математичної статистики в наукових дослідженнях” складається з одного змістового модуля: методи математичної статистики. **Метою вивчення дисципліни** «Методи математичної статистики в наукових дослідженнях» полягає у формуванні у здобувачів вміння: використовувати інформаційні технології та програмні продукти у рамках наукового дослідження використовуючи методи математичної статистики; опрацьовувати результати впровадження розроблених моделей (систем) пов’язаних з їх подальшою практичною реалізацією. **Поняттєве поле:** методи математичної статистики; статистична гіпотеза. статистичні критерії: Крамера-Уелча; Вілкоксона та Манна-Уїтні; $\chi 2$ – хі-квадрат; Фішера; t-критерій Стьюдента; алгоритм вибору статистичного критерію; параметричні критерії; вимоги до застосування параметричних критеріїв; описова статистика; статистичний взаємозв’язок результатів вимірювань; кореляція; кореляційний аналіз; щільність взаємозв’язку.	**Залік**
Алгебраїчні структури в криптографії (4 кредити, 5 семестр)	Дисципліна «Алгебраїчні структури в криптографії» передбачає вивчення алгебраїчних методів, які використовуються у різноманітних алгоритмах забезпечення захисту інформації у кіберпросторі. Завдання дисципліни полягає у набутті знань, умінь та навичок щодо використання алгебраїчних структур, методів ефективної реалізації основних алгебраїчних операцій, які дозволяють будувати як відомі криптографічні, так і нові алгоритми. **Мета вивчення дисципліни:** формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій щодо використання алгебраїчних методів створення криптографічних систем у вигляді практичних алгоритмів захисту інформації у мережах. **Поняттєве поле:** алгебраїчні структури: групоїди, напівгрупи, моноїди, групи, поля; математичні моделі на основі алгебраїчних структур; методи аналізу криптографічних систем на базі властивостей алгебраїчних операцій; криптографічні системи на основі групи точок еліптичної кривої.	**Залік**

Моделі та методи оцінювання шкоди у разі витоку інформації з обмеженим доступом (4 кредити, 1 – 2 семестри)	Дисципліна «Моделі та методи оцінювання шкоди у разі витоку інформації з обмеженим доступом» передбачає вивчення основних понять, структури, основних підходів та методів моделювання, формування умінь та навичок моделювання та оцінки моделей, достатніх для застосування і подальшого продовження самоосвіти у галузі інформаційної безпеки та захисту інформації; **Мета** вивчення дисципліни: формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно досліджувати пізнавальну та реалізовувати прогнозуючу функції щодо теорії і практики визначення основних особливостей принципів побудови сучасних моделей, методів, систем, засобів захист інформації з обмеженим доступом **Поняттєве поле:** Моделі інтегрованого представлення параметрів персональних даних, конфіденційної чи службової інформації та шкоди у разі їх витоку. Методи, системи та засоби оцінювання .	**Залік**
Штучний інтелект у кібербезпеці (4 кредити, 5 семестр)	Дисципліна «Штучний інтелект у кібербезпеці» передбачає освоєння математичного апарату ймовірнісних та детерміністських методів машинного навчання, прийняття рішень з акцентом на методи забезпечення робастності кінцевих систем на їх основі. **Мета** вивчення дисципліни: формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно аналізувати та підвищувати робастність цільових систем, аналізувати та знаходити атаки та відхиляючі приклади для цільових систем, створювати математичне та програмне забезпечення для аналізу безпеки цільових систем. **Поняттєве поле:** методи штучного інтелекту в складі SIEM систем, фреймворків безпеки, методи offensive security, генеративні моделі.	**Залік**
Безпечний дизайн програмного забезпечення (4 кредити, 5-6 семестр)	Дисципліна «Безпечний дизайн програмного забезпечення» фокусується на різних елементах, необхідних для вирішення та реалізації безпечного придбання та розробки програмного забезпечення протягом усього життєвого циклу розробки програмного забезпечення (SDLC). **Мета** вивчення дисципліни: формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно використовувати наскрізні принципи технологій (інструментів) та процесів для проектування та розробки послідовно безпечних програм. Цей курс акцентується на важливості та цінності принципу глибокоешелонованого захисту у всьому SDLC, методах адаптації спільних дій щодо безпеки до сучасних методів розробки програмного забезпечення, включаючи Agile/Scrum та DevOps. **Поняттєве поле:** захист SDLC, стандарт безпеки, дефект безпеки продукту, концепції Agile/Scrum, DevOps та ShiftLeft.	**Залік**

Управління інноваційними проектами (4 кредити, 5-6 семестр)	Дисципліна «Управління інноваційними проектами» передбачає вивчення теоретичних та практичних аспектів управління проектами з метою впровадження нововведень. Вона охоплює такі теми, як створення проектного планування, розробка бізнес-стратегії, оцінка ризиків та прийняття рішень, управління ресурсами проекту, комунікації зі зацікавленими сторонами, використання інструментів проектного менеджменту, забезпечення якості та контроль проекту. **Мета** вивчення дисципліни формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно ініціювати та управляти проектами інноваційного характеру в сфері професійної діяльності. **Поняттєве поле:** процеси управління, проекти, технології та операції, що супроводжують інноваційні проєкти, питання стратегічного планування, впровадження програм управління інформаційною безпекою моніторинг та аудит систем управління інформаційною безпекою	**Залік**
Особливості сучасної наукової комунікації (3 кредити, 3 семестр)	Дисципліна «Особливості сучасної наукової комунікації» передбачає вивчення сучасних технологій та методів комунікації, які використовуються у науковій спільноті. Це включає в себе вивчення особливостей наукової комунікації, таких як публікації наукових статей та дослідницьких звітів, взаємодії з колегами та партнерами, презентації досліджень, а також використання сучасних технологій для підвищення ефективності наукової комунікації. **Мета** вивчення дисципліни у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно організовувати цифрову наукову комунікацію, відкритий доступ, відкриту науку, відкриті ліцензії, управління даними досліджень, вплив на життєвий цикл наукового дослідження, зокрема, у поширенні та збереженні результатів наукового дослідження. Застосовувати сучасні практики та пошукові техніки для роботи з науковими джерелами, використовувати універсальні та спеціалізовані інформаційні ресурси, сучасні веб-застосунки для різних етапів дослідження і не тільки. Загальний огляд основних складників та стратегій наукової комунікації, використання сучасних веб-застосунків на всіх етапах життєвого циклу дослідження, особливо під час пошуку інформації та поширення результатів дослідження. **Поняттєве поле:** Наукова інформація, спеціалізовані пошукові системи та бази даних, стратегії ефективного пошуку в інтернеті, інструменти моніторингу нових публікацій з проблематики дослідження, наукова стаття в рецензованому журналі – основна одиниця наукової комунікації, публікаційна стратегія наукометрії та бібліометрії, авторське право.	**Залік**