МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Мілов О. В., к.т.н., проф. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Дисципліна «Математичні основи криптології» забезпечує підготовку бакалаврів відповідно до вимог і навчального плану спеціальності «Кібербезпека», ознайомлення студентів з математичними основами криптології, а саме – основами теорії чисел, лінійною алгеброю, основами дискретної математики, комбінаторики та ін. Дисципліна «Математичні основи криптології» розглядається як теоретична і прикладна дисципліна, що дає уявлення про основні математичні методи та підходи, що застосовуються для забезпечення криптографічного захисту інформації в процесі зберігання та передачі інформації, представленої в двійкових кодах. Дисципліна присвячена вивченню математичних основ криптології та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах. Дисципліна розкриває поняття шифрів, симетричної та асиметричної криптографії, електронного підпису, гешування та інші математичні об'єкти криптографії. Вивчаються відповідні криптографічні стандарти, що застосовуються сьогодні в захисті інформації в Україні та за кордоном. Докладно розглядаються: стандарти RSA. DES. GOST1989. та інші. Також приділено увагу перспективним напрямам в криптології: криптографічним протоколам з розголошенням і без розголошення, теорії алгоритмічної складності і одностороннім функціям, схемам поділу секрету і деяким їх застосуванням в задачах ідентифікації і аутентифікації.

Метою вивчення дисципліни «Математичні основи криптології» є ознайомлення з основами математичної теорії криптології.

Результатами навчання є придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації, розуміння суті інформаційних процесів в криптографічних системах, навички застосування комп'ютерів для вирішення завдань шифрування і дешифрування та навички розробки і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Характеристика навчальної дисципліни

Курс	**2**
Семестр	**3**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Математичний аналіз Лінійна алгебра Теорія ймовірностей і математична статистика Дискретна математика Інформатика Програмування	Основи криптографічного захисту

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

	РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	РН–10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН–11. виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–15. використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20. забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–31. застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

(автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25. 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; РН–26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34. приймати участь у розробці та впровадженні стратегії

	інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35. 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; РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовій модуль 1. Традиційне шифрування

Тема 1. Цілі підтримки безпеки. Атаки, послуги та механізми.
Тема 2. Модульна арифметика. Шифрувальні машини.
Тема 3. Матриці.
Тема 4. Традиційні шифри з симетричним ключем
Тема 5. Алгебраїчні структури.
Тема 6. Сучасні блокові шифри.

Змістовій модуль 2. Сучасні методи шифрування

Тема 7. Перетворення.
Тема 8. Розширення ключів.
Тема 9. Застосування сучасних блокових шифрів.
Тема 10. Прості числа.
Тема 11. Квадратичне порівняння з модулем.
Тема 12. Криптографічна система RSA..

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові міні-проекти.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- застосовувати найпростіші шифри;
- обирати згідно з технічною необхідінстю блокові симетричні шифри;
- використовувати Асиметричні криптосистеми;
- використовувати Pretty Good Privacy;
- застосовувати стеганографічні методи захисту інформації;
- застосовувати пакет NIST. HASH Analyzer.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 12 (робота на лекціях).

Лабораторні заняття: максимальна кількість балів становить 88 (виконання лабораторних робіт – 48, контрольні роботи – 40), а мінімальна – 54.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Лекція *"Цілі підтримки безпеки. Атаки, послуги та механізми."*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1 Основи роботи з MS Word*	Виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *" Модульна арифметика.шифрувальні машини"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1 (продовження) Основи роботи з MS Word	Виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Матриці"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2. Основи роботи з MS Excel	Виконання лабораторної	4

			роботи	
			Контрольна робота 1	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Традиційні шифри з симетричним ключем"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 (продовження). Основи роботи з MS Excel	Виконання лабораторної роботи	4
Тема 5	***Аудиторна робота***			
	Лекція	Лекція*"Алгоритми"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3.Основи роботи з MS PowerPoint	Виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Сучасні блокові шифри"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6. *"Початок роботи консолі за допомогою програми Tera Term"*	Виконання лабораторної роботи	4
			Контрольна робота 2	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Перетворення"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4.	Виконання лабораторної роботи	4
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Розширення ключів"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4. (продовження)	Виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Застосування сучасних блокових шифрів"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5.	Виконання лабораторної роботи	4
			Контрольна робота 2	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Прості числа"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5 (продовження).	Виконання лабораторної роботи	4
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 11	***Аудиторна робота***			
	Лекція	Лекція *"Квадратичне порівняння з модулем.*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6.	Виконання лабораторної роботи	4
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 12	***Аудиторна робота***			
	Лекція	Лекція *"Криптографічна система RSA"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №6 (продовження).	Виконання лабораторної роботи	4
			Контрольна робота 3	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005, Д 85с.

2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009

3. Бирюков А. А. Информационная безопасность: защита и нападение - М.: ДМК Пресс, 2012

Додаткова

4. Вернет, Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином, 2002,342с.

5. Виега Д., Лебланк Д., Ховард М. 19 смертных грехов, угрожающих безопасности программ : Как не допустить типичных ошибок - М.: ДМК Пресс, 2009 v

6. Грэм, Кнут, Паташник. Конкретная математика. - М.: Мир, 1998, 145с.

7. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. Программно-аппаратные средства обеспечения информационной безопасности. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000, 176с.

8. А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах. - М.: Горячая Линия - Телеком, 2001, 126с.

9. А.А. Молдовян, Н.А. Молдовян, Гуц, Изотов. - Криптография: скоростные шифры. - СПб.: БХВ, 2002, 222 с.

10. Ноден, Ките. Алгебраическая алгоритмика. - М.: Мир, 1999, 192с.

Інформаційні ресурси

11. www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби.

12. www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою.

13. www.itsec.ru - Інтернет-журнал «Інформаційна безпека».

14. www.inside-zi.ru - Інформаційно-методичний журнал «Захист інформації. Інсайд».

15. www.kaspersky.ru - Лабораторія Касперського.

16. www.drweb.com – Лабораторія DrWeb.

17. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної

дисципліни “Математичні основи криптології” https://pns.hneu.edu.ua/course/view.php?id=5678