Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми _ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА
(назва)

Освітнього рівня **першого (бакалаврського) рівня вищої освіти**

Спеціальності **125 “Кібербезпека”**

Галузь знань **12 “Інформаційні технології”**

1. Назва освітньої компоненти **Прикладна криптологія**
(назва дисципліни)

2. Тип **основна**

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	8	240	36	-	36	72	96
4. Взаємозв’язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Вища математика. 2. Теорія інформації та кодування. 3.Операційні системи. 4.Стандарти інформаційної та кібербезпеки. 5.Комп’ютерні мережі.						
Освітні компоненти для яких є базовою	1. Технічні засоби захисту інформації. 2. Основи захисту комп’ютерних мереж. 3. Інфраструктура відкритих ключів. 4. Стандарти крипторгафічного захисту. 5. Курсова робота і бакалаврська робота.						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Сучасні криптографічні алгоритми блокового і потокового			1.Проектувати блокові й потокові шифри із потрібними				

шифрування;	характеристиками;
2. Сучасні криптографічні алгоритми з відкритими ключами;	2.Вибирати ключі для алгоритмів асиметричного шифрування;
3.Особливості реалізації цифрового підпису і хеш-функцій;	3.Оцінювати стійкість шифрів;
4. Протоколи автентифікації і розподілу ключової інформації;	4.Здійснювати вибір криптопротоколів згідно з вимогами конкретного застосування;
5. Відомі методи аналізу криптосистем та тенденції розвитку криптографії та криптоаналізу;	5.Розробляти програмні та апаратні засоби, що реалізують криптоалгоритми і криптопротоколи;
6.Особливості практичного використання криптографічних протоколів.	6. Практично застосовувати відомі програмні засоби криптографічного захисту інформації.
Компетенції відповідно до вимог роботодавців	
1. Знати загальну методику організації підсистем криптографічного захисту інформації в комп'ютерних системах та мережах;	1.Характеризувати сучасні системи криптографічного захисту інформації;
2. Орієнтуватися в термінології й формулюваннях теоретичних результатів відносно стійкості сучасних криптографічних систем;	2.Використовувати професійно профільовані знання й практичні навички в галузі математики для освоєння прикладної криптології;
3. Використовувати загальні принципи побудови систем криптографічного захисту інформації;	3. Використовувати методи криптографічних перетворень інформації та способи їх здійснення при симетричному і асиметричному шифруванні;
4. Методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;	4. Аналізувати криптографічні протоколи на їх рівень безпечності (повноту, коректність та нульове розголошення таємниці тощо);
5. Методи автентифікації інформації. Геш-функції. Проблема захисту від модифікування даних;	5. Застосовувати основні методи криптоаналізу односторонніх геш-функцій.
6. Життєвий цикл ключів. Поняття про ключову систему;	6.Застосовувати протоколи транспортування та узгодження ключів. Перетворення ключів.
7. Поняття про електронний цифровий підпис (ЕЦП). Призначення, застосування, властивості і вимоги до ЕЦП.	7. Застосовувати і розробляти загальні схеми побудови ЕЦП.

6. Результати навчання відповідно до ОПП						
Знання та розуміння предметної області та розуміння професії. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.						
7. План вивчення освітньої компоненти						
Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1 *Математичні основи криптології* (5.ПФ.Д.04 ПП О 01.01 Б, Т)						
	Лекція 1	Тема: Теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії.	1.Поняття теорії чисел. 2.Поняття скінченних полів Галуа.	Застосовувати в криптографії теорію чисел і скінченні поляГалуа.		http://dl.dut.edu.ua/mod/resource/view.php?id=64588
	Лекція 2	Тема: Еліптичні та гіпереліптичні групи, основи застосування в криптології.	Поняття еліптичних та гіпереліптичних кривих.	Застосовувати еліптичні та гіпереліптичні групи в криптології.		http://dl.dut.edu.ua/mod/resource/view.php?id=84102
	Лекція 3	Тема:Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптології.	Поняття бінарних відображень (спарювання) точок еліптичних кривих	Застосовувати відображення (спарювання) точок еліптичних кривих в криптології.		http://dl.dut.edu.ua/mod/resource/view.php?id=64589

Розділ 2 *Симетричні криптографічні системи* (5.ПФ.Д.04 ПП О 01.02 Б, Т)						
	Лекція 4	Тема:Симетричні крип-тографічні перетворення та їх властивості.	Блокові та потокові симетричні шифри.	Розробляти нові та використовувати відомі шифри.		http://dl.dut.edu.ua/mod/resource/view.php?id=64590
	Лекція 5	Тема: Джерела ключів та ключової інформації, вимоги до них.	Основні правила зберігання ключів.	Правила розповсюдження ключів.		http://dl.dut.edu.ua/mod/resource/view.php?id=64599
Розділ 3 *Асиметричні криптографічні системи* (5.ПФ.Д.04 ПП О 01.03 Б, Т)						
	Лекція 6	Тема: Вступ в теорію асиметричних крипто перетворень.	Перелік та загальну характеристика асиметричних крипто перетворень.	Проблемні питання крипто перетворень типу RSA.		http://dl.dut.edu.ua/mod/resource/view.php?id=64600
	Лекція 7	Тема:Асиметричні крипто перетворення в групах точок еліптичних кривих.	Переваги крипто перетворення НШ в групі точок еліптичної кривої.	Правила генерування асиметричної ключової пари в групах точок еліптичних кривих.		http://dl.dut.edu.ua/mod/resource/view.php?id=84124
Розділ 4 *Методи автентифікації інформації* (5.ПФ.Д.04 ПП О 01.04 Б, Т)						
	Лекція 8	Тема:Методи та механізми автентифікації в криптосистемах.	Поняття: Ідентифікація. Автентифікація користувача. Автентифікація мережі.	Правила використання протоколу автентифікації.		http://dl.dut.edu.ua/mod/resource/view.php?id=84127
	Лекція 9	Тема: Методи та механізми захисту від несанкціонованого доступу.	Рівні моделі порушника.	Правила визначення персональних даних. Закон України «Про захист персональних даних».		http://dl.dut.edu.ua/mod/resource/view.php?id=84131
Розділ 5 *Цифровий підпис та його властивості*(5.ПФ.Д.04 ПП О 01.05 Б, Т)						
	Лекція 10	Тема: Електронні цифрові підписи з додатком.	Вимоги до ЕЦП з додатком.	Застосовувати електронні цифрові підписи з додатком.		http://dl.dut.edu.ua/mod/resource/view.php?id=84135

	Лекція 11	Тема: Електронні цифрові підписи з відновлення повідомлень.	Сутність, властивості та області застосування ЦП з відновленням повідомлення.	Виконувати процес обчислення підпису.		http://dl.dut.edu.ua/mod/resource/view.php?id=64610
	Лекція 12	Тема: Властивості та основи застосування електронних цифрових підписів.	Схеми підпису, що розглядаються, дозволяють відновлювати повідомлення у змісті відновлення деяких з даних, що використовуються при обчисленні підпису.	Генерувати (обчислювати) ключ сеансу і попереднього ЦП.		http://dl.dut.edu.ua/mod/resource/view.php?id=84144
Розділ 6 *Криптографічні протоколи* (5.ПФ.Д.04 ПП О 01.06 Б, Т)						
	Лекція 13	Тема: Криптографічні механізми та протоколи управління ключами.	Визначення та класифікація криптографічних протоколів.	Способи класифікації протоколівзалежно від їхнього функціонального призначення тощо.		http://dl.dut.edu.ua/mod/resource/view.php?id=64613
	Лекція 14	Тема: Квантова криптографія та крипто аналіз.	Основні фундаментальні властивості квантових систем, які використовуються в квантовій криптографії.	Протоколи квантового поширення ключа.		http://dl.dut.edu.ua/mod/resource/view.php?id=84145
Розділ 7 *Криптографічний аналіз асиметричних криптосистем* (5.ПФ.Д.04 ПП О 02.01 Б, Т)						
	Лекція 15	Тема: Методи крипто аналізу асиметричних криптосистем.	Основні методи крипто аналізу асиметричних криптосистем.	Способи визначення особистого(таємного) ключа із ключової пари.		http://dl.dut.edu.ua/mod/resource/view.php?id=84147
	Лекція 16	Тема: Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих.	Поняття еліптичної кривої над полем Галуа та метрика арифметичних операцій.	Побудова загальносистемних параметрів ЕК.		http://dl.dut.edu.ua/mod/resource/view.php?id=84148
Розділ 8 *Криптографічний аналіз симетричних криптосистем* (5.ПФ.Д.04 ПП О 02.01 Б, Т)						
	Лекція 17	Тема: Вступ в теорію	Основні погрози безпеки	Реалізація		http://dl.dut.e

		крипто аналізу в симетричних криптосистемах.	інформації.	криптографічних перетворень з чотирма рівнями стійкості.		du.ua/mod/resource/view.php?id=64616
	Лекція 18	Тема: Методи крипто аналізу блокових симетричних криптосистем.	Поняття безумовно та обчислювально стійких криптосистем.	Навести приклад формування гами шифрування.		http://dl.dut.edu.ua/mod/resource/view.php?id=64616

Практичні заняття						
	Практичне заняття 1	Тема: Аналіз методів скалярного множення в групі точок еліптичних кривих, афінне та проективне подання точок еліптичних кривих, порівняльний аналіз складності операцій додавання та подвоєння точок еліптичних кривих для різних подань	Визначення базової точки ЕК.	Запишіть та поясніть формулу подвоєння точок еліптичної кривої над простим полем.		http://dl.dut.edu.ua/mod/resource/view.php?id=64591
	Практичне заняття 2	Тема: Аналіз методів криптографічних перетворень, критерії та показники оцінки якості крипто перетворень, умови реалізації безумовно стійких, обчислювально стійких та ймовірно стійких шифрів.	Якими властивостями володіють безумовно стійкі криптоалгоритми	Дайте визначення підстановки та назвіть її властивості.		http://dl.dut.edu.ua/mod/resource/view.php?id=84104
	Практичне заняття 3	Тема: Аналіз методів симетричних крипто перетворень, блокові та потокові симетричні шифри та методичні основи їх порівняння. Елементарні шифри та їх властивості.	Яка послідовність вважається випадковою? Дайте визначення потокового шифру та зробіть перелік його основних властивостей.	Сформулюйте вимоги до таблиць перетворень, що застосовуються в FIPS-197. Зробіть класифікацію потокових шифрів.		http://dl.dut.edu.ua/mod/resource/view.php?id=64601

	Практичне заняття 4	Тема: Аналіз асиметричних криптографічних перетворень. Моделі загроз та порушника. Синтез крипто перетворень в скінченних полях та кільцях. Направлені шифри та їх реалізація.	Найбільша загрозливість для криптоперетворень в простих полях. Сутність атаки типу універсальне розкриття.	Вимоги до модулів перетворень в полях Галуа. Розробіть алгоритм формування загальносистемних параметрів $\{P, a\}$. Поясніть алгоритм виробки загального секрету, що здійснюється з використанням довгострокових ключів.		http://dl.dut.edu.ua/mod/resource/view.php?id=84142
	Практичне заняття 5	Тема: Аналіз асиметричних крипто перетворень в групах точок еліптичних кривих над скінченними полями. Афінні та проективні подання, порівняння властивостей.	Основні задачі криптоаналізу для систем, в яких перетворення здійснюються в групі точок ЕК, методи їх розв'язання та оцінка стійкості для відомих методів криптоаналізу.	Назвіть та порівняйте складність основних методів розв'язку дискретних логарифмічних рівнянь в групі точок ЕК. Сутність методу $\rho -$Поларда розв'язку дискретного логарифмічного рівняння в групі точок ЕК.		http://dl.dut.edu.ua/mod/resource/view.php?id=84143
	Практичне заняття 6	Тема: Методи генерування випадкових та псевдовипадкових послідовностей. Детерміновані генератори псевдовипадкових послідовностей. Вимоги до генераторів ключів та ключової інформації.	Поясніть схему генератора випадкових послідовностей з одним або двома каналами формування випадкових бітів. Яка послідовність вважається випадковою? Чим відрізняється випадкова послідовність від псевдовипадкової?	Сформулюйте вимоги до ключа (блоку) заміни, що використовується в ГОСТ-28147-89. Сформулюйте вимоги до ключа (блоку) заміни, що використовується в ГОСТ-34.311-95.		http://dl.dut.edu.ua/mod/resource/view.php?id=64611
	Практичне заняття 7	Тема: Аналіз загроз обману. Методи забезпечення цілісності та справжності	Для чого здійснюється автентифікація повідомлень? Як здійснити виробку	Визначте поняття цілісності та справжності, яким чином вони		http://dl.dut.edu.ua/mod/resource/view.p

		інформації при застосуванні симетричних криптоперетворень. Методи захисту від несанкціонованого доступу.	імітовкладки з використанням симетричного криптоалгоритму?	забезпечуються? В чому суть парадоксу дня народження?		hp?id=84146
	Практичне заняття 8	Тема: Класифікація цифрових підписів. Цифрові підписи з додатком. Основні загрози та протидія їм. Оцінка стійкості цифрових підписів з додатком. Стандартизація цифрових підписів з додатком.	Класифікація та методи здійснення ЕЦП з додатком	Методи виконання ЕЦП з додатком Електронні цифрові підписи з додатком в групі точок ЕК та їх властивості		http://dl.dut.edu.ua/mod/resource/view.php?id=84169
	Практичне заняття 9	Тема:Цифрові підписи з відновленням повідомлень. Оцінка стійкості цифрових підписів з відновленням повідомлень. Стандартизація цифрових підписів з відновленням повідомлень.	Сутність, властивості та області застосування ЦП з відновленням повідомлення	Яким чином мають формуватись загальносистемні параметри та ключі ЕЦП? Порівняйте властивості та захищеність від можливих атак на ЕЦП ISO-15946-2 (ECDSA, EC GDSA, EC KC DSA)?		http://dl.dut.edu.ua/mod/resource/view.php?id=64592
	Практичне заняття 10	Тема:Аналіз протоколів управління ключами. Основні механізми та протоколи. Критерії та показники оцінки та порівняльного аналізу. Стандартизація протоколів управління ключами.	Моделі інтерактивного та протоколу з нульовими знаннями.	В чому сутність інтерактивного протоколу з нульовими значеннями? Поясніть сутність протоколу Діффі-Хеллмана. Поясніть сутність слушного протоколу при використанні RSA криптоперетворень. .		http://dl.dut.edu.ua/mod/resource/view.php?id=84103

	Практичне заняття 11	Тема: Криптографічні механізми та протоколи автентифікації. Протоколи автентифікації з використанням симетричних та асиметричних крипто перетворень. Інтерактивні та протоколи з нульовим розголошенням.	Механізми автентифікації, що не потребують залучення третьої довіреної сторони. Механізми автентифікації що ґрунтуються на криптографічній контрольній сумі.	Механізми узгодження ключів, що не включені в стандарт управління ключами ISO/IEC 11770-3. Механізми передавання ключів.		http://dl.dut.edu.ua/mod/resource/view.php?id=64602
	Практичне заняття 12	Тема: Методи та системи крипто аналізу асиметричних криптосистем. Складність криптоаналізу перетворень типу цифровий підпис та направлене шифрування групі точок еліптичних кривих.	Криптоаналіз RSA методом квадратичного решета. Приклади розв'язку задач та задачі для самостійного розв'язання.	Порівняйте складність криптоаналізу RSA, якщо використовуються метод ρ –Полларда, метод Ленстри, квадратичне решето та загальне решето числового поля.		http://dl.dut.edu.ua/mod/resource/view.php?id=64601
	Практичне заняття 13	Тема: Методи криптоаналізу симетричних шифрів. Оцінка стійкості блочних симетричних шифрів. Криптоаналітичні системи та їх застосування.	Механізми автентифікації, що потребують залучення третьої довіреної сторони	Однобічна автентифікація з декількома проходами. Взаємна автентифікація. Основні завдання криптоаналізу, як розділу криптології.		http://dl.dut.edu.ua/mod/resource/view.php?id=84156
Теми лабораторних робіт						
	Лабораторне заняття 1	Тема:Джерела ключів. Методи та засоби формування випадкових та псевдовипадкових послідовностей. Дослідження властивостей випадкових та псевдовипадкових послідовностей.	Методика тестування ГВЧ і ГПВЧ на основі критеріїв а стандартів FIPS 140-1 та AIS – 20(31).	Архіватори як джерела псевдовипадкових чисел.		http://dl.dut.edu.ua/mod/resource/view.php?id=64592

	Лабораторне заняття 2	Тема: Дослідження властивостей симетричних крипто перетворень. Методи та засоби генерування ключів в симетричних криптосистемах.	Вивчення побудови та застосування симетричних крипто перетворень(шифрів)	Дослідження статистичних властивостей класичних та сучасних систем. Порівняльний аналіз сучасних та класичних симетричних шифрів.		http://dl.dut.edu.ua/mod/resource/view.php?id=64594
	Лабораторне заняття 3	Тема:Дослідження властивостей асиметричних крипто перетворень в групі точок еліптичних кривих.	Побудова ключів для асиметричної криптографії	Методи факторизації модуля		http://dl.dut.edu.ua/mod/resource/view.php?id=64603
	Лабораторне заняття 4	Тема: вимоги, сутність, методи побудови, порядок аналізу властивостей, принципи реалізації та основні сфери застосування протоколів узгодження ключів.	Протокол узгодження ключів типу Діффі-Геллмана з двома електронними цифровими підписами та підтвердженням ключів	Основні формули та параметри для застосування криптографічного протоколу узгодження ключів.		http://dl.dut.edu.ua/mod/resource/view.php?id=64604
	Лабораторне заняття 5	Тема: Розроблення програмних моделей та дослідження перспективних криптографічних перетворень типу електронний цифровий підпис.	Підпис документу з використанням алгоритмів на еліптичних кривих.	Порівняння обчислювальної складності вироблення і перевірки ЕЦП алгоритмів ЕЦП Шнора, та ECSS.		http://dl.dut.edu.ua/mod/resource/view.php?id=64605
	Лабораторне заняття 6	Тема: Протоколи розподілу таємниці. Класифікація та вимоги до протоколів розподілу таємниці. Методи розподілу та підтвердження таємниці. Синтез та	Вивчення та дослідження криптографічних протоколів розподілення таємниці.	Протокол розділення таємниці Шаміра. Протокол розділення таємниці за допомогою КТЗ (Китайської теореми про залишки).		http://dl.dut.edu.ua/mod/resource/view.php?id=64612

		аналіз криптографічних протоколів.				
	Лабораторне заняття 7	Тема: Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих.	Основні методики криптоаналізу у криптосистемах з відкритим ключем, зокрема метод факторизації та атаки для RSA- перетворень.	Атака типу «груба сила» або метод повного перебору		http://dl.dut.edu.ua/mod/resource/view.php?id=64614
Самостійна робота						
Розділ 1		Тема: Математичні основи криптології.	Скінченні поля Галуа. Еліптичні криві.	Факторизація модуля – складеного цілого великого числа. Методи перетворень у групі точок ЕК, що використовуються на практиці або є перспективними.		
Розділ 2		Тема: Симетричні криптографічні системи.	Основні завдання криптографії. Базові криптографічні послуги.	Класифікація симетричних криптографічних перетворень.		
Розділ 3		Тема: Асиметричні криптографічні системи.	Криптоперетворення направленого шифрування (НШ) в полі Галуа. Криптоперетворення НШ в групі точок еліптичних кривих.	Управління асиметричною парою ключів.		
Розділ 4		Тема:Методи автен-тифікації інформації.	Структурна схема і математична модель захищеної інформаційно-телекомунікаційної системи (ІТС).	Поняття ідентифікації та автентифікації користувача, мережі, повідомлень, інформації (ресурсів).		
Розділ 5		Тема:Цифровий підпис та його властивості.	Основні положення і характеристики ЦП. Основні послуги та застосування ЦП.	Класифікація ЦП. Вимоги до ЦП з додатком. Асиметричні		

				криптографічні перетворення для ЦП. Основні види атак на ЦП.		
Розділ 6		Тема: Криптографічні протоколи.	Визначення та класифікація криптографічних протоколів.	Моделі оцінки та умови безпеки протоколів. Протокол Діффі-Геллмана, сутність та умови реалізації різними методами.		
Розділ 7		Тема:Криптографічний аналіз асиметричних криптосистем.	Сутність та класифікація методів криптоаналізу асиметричних криптосистем	Методи криптоаналізу RSA криптосистем.		
Розділ 8		Тема:Криптографічний аналіз симетричних криптосистем.	Основні функції систем криптоаналізу. Класифікація та попередня оцінка сучасних методів криптоаналізу блокових симетричних шифрів.	На які класи діляться шифри за криптографічною стійкістю. Типи криптоаналітичних атак.		
Розділ 9		Тема:Виконання курсової роботи.	Згідно навчального плану	Згідно навчального плану		

8. Мова вивчення освітньої компоненти

(українська, англійська, розділи, що викладаються англійською мовою)

Українська

9. Інформаційне забезпечення освітньої компоненти

Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела

1.Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.
2.Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 1 видання, 878 с.
3.Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2012 р.
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.Katz J., Lindell Y. Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) 2nd Edition. CRC Press, 2015. – 583p.
7.Імітаційне моделювання систем масового обслуговування / [В.Б. Толубко, А.Д. Кожухівський, В.В. Вишнівський, Г.І. Гайдур, О.А. Кожухівська].-Навч. посібник (Електронне видання).-К.: ДУТ.-2018.- 175 с.

10. Методи оцінювання, підсумкові звітності за освітньою компонентою

(заліки, екзамени, курсові проекти, тестування)

Заліки, екзамени, курсові роботи, тестування

11. Матеріально-технічне забезпечення освітньої компоненти

11.1 Навчально-методичне забезпечення

Програма та робоча програма навчальної дисципліни. Плани лекцій. Методичні рекомендації до проведення практичних та лабораторних занять. Дидактичне забезпечення самостійної роботи студентів. Матеріали комплексної контрольної роботи (ректорські контрольні роботи). Затверджені питання на модульний контроль. Затверджені питання до заліку та екзамену. Методичні рекомендації для студентів заоч.ф.н. та завдання. Критерії оцінювання знань. Інформаційно-навчальні матеріали для студентів на навчальному сайті. Перелік навчально-методичних посібників (основна література).

11.2 Навчально-матеріальне забезпечення

Лабораторія 419, 421

Програмне забезпечення

Програмне забезпечення CrypTool,