Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Навчально-науковий Фізико-Технічний інститут
Кафедра інформаційної безпеки

ОСНОВИ КРИПТОГРАФІЇ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Обов'язкова (Нормативна)*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*II рік підготовки, весняний семестр*
Обсяг дисципліни	*2 кредити ECTS*
Семестровий контроль / контрольні заходи	*Залік / Модульна контрольна робота/ Розрахункова робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції, практичні заняття: Микола КОНОТОПЕЦЬ*
Розміщення курсу	*Google Classroom*

Київ 2022

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента «Основи криптографії» складено відповідно до освітньої програми підготовки бакалаврів «Комп'ютерні системи і технології спеціального зв'язку» спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у курсантів наступних компетентностей: (ЗК1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК2) Здатність застосовувати знання у практичних ситуаціях; (ЗК6) Здатність вчитися й оволодівати сучасними знаннями; (ЗК11) Здатність приймати обґрунтовані рішення; (ЗК12) Здатність оцінювати та забезпечувати якість виконуваних робіт; (СК1) Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування.

Предмет навчальної дисципліни – основні державні та зарубіжні стандарти криптографічного захисту інформації, практичне використання отриманих знань для синтезу та аналізу симетричних та асиметричних криптографічних систем.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР1) Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР2) Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації; (ПР16) Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни курсант повинен володіти освітніми компонентами «Основи теорії інформації та кодування». Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента є необхідними для подальшого вивчення освітніх компонентів «Засоби і комплекси криптографічного захисту інформації».

3. Зміст навчальної дисципліни

Семестр 4

Семестровий (кредитний) модуль 1. Основи криптографії.

Тема 1. Математичні основи криптографії

Заняття: Роль та місце криптографії в сфері інформаційної безпеки. Предмет і задачі криптографії. Основи алгебри та теорії чисел. Розв'язання завдань на подільність цілих чисел. Алгоритм Евкліда.

Тема 2. Принципи побудови та аналізу симетричних криптографічних систем

Заняття: Потокові криптосистеми. Блокові криптосистеми. Міжнародні та національні стандарти симетричних криптографічних систем. Розв'язання завдань на дослідження основних властивостей ЛРЗ. Розв'язання завдань на дослідження властивостей елементів сучасних потокових та блокових шифрів.

Тема 3. Принципи побудови та аналізу асиметричних криптографічних систем

Заняття: Основні етапи розвитку та напрямки застосування асиметричної криптографії. Асиметричні протоколи розподілу ключів. Цифровий підпис. Протоколи узгодження ключів для конференц-зв'язку (групи користувачів). Розв'язання завдань на дослідження властивостей криптографічної системи RSA. Розв'язання завдань на дослідження властивостей криптографічної системи Ель-Гамаля.

Тема 4. Застосування криптографічних алгоритмів та протоколів для захисту інформації

Заняття: Криптографічні ґеш-функції. Автентифікація об’єкту. Основні підходи до управління ключами. Побудова, аналіз стійкості та застосування криптографічних геш-функцій. Перспективні напрями розвитку криптографії.

4. Навчальні матеріали та ресурси

Основна література:

1. Олексійчук А.М., Конюшок С.М., Проскуровський Р.В. Засоби та комплекси криптографічного захисту інформації. Частина 1. Вступ до теорії булевих функцій та її криптографічних застосувань: Навчальний посібник. – К.: ІССЗІ НТУУ "КПІ", 2012. – 182 с., іл.
2. Ковальчук Л.В., Конюшок С.М., Кучинська Н.В. Прикладна алгебра: основні поняття алгебри та теорії чисел: Електрон. навч. посібник. – К.: НТУУ "КПІ", 2011. – 178 с. (з грифом "Рекомендовано Методичною радою НТУУ "КПІ" від 17.03.2011 р., протокол № 7).
3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. – Харків: видавництво "Форт", 2012. – 880 с.
4. Вербицький О. В. Вступ до криптології. – Львів.: ВНТЛ., 1998. – 248 с.
5. Глинчук Л.Я. Г 54 Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
6. Національний стандарт України ДСТУ 7624:2014. Алгоритм симетричного блокового перетворення.
7. Національний стандарт України ДСТУ 7564:2014. Функція хешування.
8. Національний стандарт України ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення.

Додаткова література:

1. Лагун А.Е. Криптографічні системи та протоколи: Навчальний посібник – Львів: Видавництво Львівська політехніка, 2013. – 96 с.
2. Завадська Л.О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006 – 54с.
3. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 2. Теорія чисел. – Вінниця: ВНТУ, 2017 – 129 с.
4. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія. – К.: 2002. – 504 с.
5. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації. – К.: Вища школа, 2002. – 457 с.
6. Бакалинський О.О., Головань С.М., Конюшок С.М. Нормативно-правове забезпечення міжнародної діяльності у сфері захисту інформації з обмеженим доступом. Практикум: Навчальний посібник. – К.: ІССЗІ НТУУ "КПІ", 2015. – 321 с. (з грифом "Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів, які навчаються за напрямом підготовки "Управління інформаційною безпекою", лист № 1/11 – 19277 від 08.12.2014 р.).
7. Корченко, Олександр Григорович. Прикладна криптологія: системи шифрування : підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс ; Міністерство освіти і науки України, Житомирський військовий інститут імені С.П. Корольова Державного університету телекомунікацій. – Житомир : [б. в.] ; 2014. - 447 с.
8. Фаль, Олексій Михайлович. Криптографія: основні ідеї та застосування : Препринт / О.М. Фаль. - К. : Політехніка, 2003. - 28 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Методика опанування навчальної дисципліни (освітнього компонента) передбачає висвітлення інформації за розділами, темами, про всі навчальні заняття (лекції, практичні) та надання рекомендацій щодо їх засвоєння (наприклад, у формі календарного плану чи деталізованого опису кожного заняття та запланованої роботи).

Самостійна робота курсанта містить інформацію про:

Види самостійної роботи (підготовка до аудиторних занять, розв'язок задач, виконання розрахункової роботи, тощо).

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин			
		Всього	у тому числі		
			Лекції	Практичні (семінарські) заняття	СРК
Тема 1	**Математичні основи криптографії**	**11,6**	**6**	**4**	**1,6**
Заняття 1/1	Роль та місце криптографії в сфері інформаційної безпеки. 1. Цілі підтримки інформаційної безпеки. 2. Загальні поняття та означення. Основна література: [3] Допоміжна література: [6]	**2,2**	2		0,2
Заняття 1/2	Предмет і задачі криптографії. 1. Основні поняття криптології. 2. Історичний аспект розвитку криптографії. 3. Основні проблеми безпеки інформації. 4. Основні класи криптографічних систем. Основна література: [4, 5] Допоміжна література: [1]	**2,2**	2		0,2
Заняття 1/3	Основи алгебри та теорії чисел 1. Арифметика цілих чисел. 2. Алгоритм Евкліда обчислення найбільшого спільного дільника. 3. Загальні алгебраїчні структури та їх властивості. Основна література: [1, 2] Допоміжна література: [2]	**2,2**	2		0,2
Заняття 1/4	Розв'язання завдань на подільність цілих чисел. 1. Подільність з остачею та конгруенції за натуральним модулем. 2. Розв'язання завдань обчислення суми та добутку цілих чисел за натуральним модулем. Основна література: [2] Допоміжна література: [3]	**2,5**		2	0,5
Заняття 1/5	Алгоритм Евкліда. 1. Практичне використання алгоритму Евкліда для перевірки умови взаємної простоти цілих чисел. 2. Розв'язання завдань обчислення найбільшого спільного дільника з використанням алгоритму Евкліда. Основна література: [2] Допоміжна література: [3]	**2,5**		2	0,5
Тема 2	**Принципи побудови та аналізу симетричних криптографічних систем**	**11,6**	**6**	**4**	**1,6**
Заняття 2/1	Потокові криптосистеми. 1. Основні принципи побудови потокових криптосистем. 2. Класифікація сучасних генераторів псевдовипадкових послідовностей. Основна література: [5] Допоміжна література: [4]	**2,2**	2		0,2

Заняття 2/2	Блокові криптосистеми. 1. Модель ітеративного блокового шифру. 2. Класифікація сучасних блокових шифрів. 3. Режими роботи блокових шифрів. Основна література: [3, 6] Допоміжна література: [7]	**2,2**	2		0,2
Заняття 2/3	Міжнародні та національні стандарти симетричних криптографічних систем 1. Основні відомості про міжнародні та національні стандарти потокового шифрування. 2. Основні відомості про міжнародні та національні стандарти блокового шифрування. Основна література: [6, 8] Допоміжна література: [8]	**2,2**	2		0,2
Заняття 2/4	Розв'язання завдань на дослідження основних властивостей ЛРЗ. 1. Математична модель лінійного регістру зсуву (ЛРЗ). 2. Основні властивості ЛРЗ. Основна література: [2] Допоміжна література: [2]	**2,5**		2	0,5
Заняття 2/5	Розв'язання завдань на дослідження властивостей елементів сучасних потокових та блокових шифрів 1. Розв'язання завдань на дослідження властивостей елементів сучасних потокових шифрів. 2. Розв'язання завдань на дослідження властивостей ЛРЗ. Основна література: [1] Допоміжна література: [5]	**2,5**		2	0,5
Тема 3	**Принципи побудови та аналізу асиметричних криптографічних систем**	**11,9**	**4**	**6**	**1,9**
Заняття 3/1	Основні етапи розвитку та напрямки застосування асиметричної криптографії. 1. Етапи створення та розвитку асиметричних криптосистем. Основні класи задач, що вирішуються з використанням асиметричних криптографічних систем. 3. Криптосистеми RSA та Ель-Гамаля Основна література: [5]. Допоміжна література: [7]	**2,2**	2		0,2
Заняття 3/2	Асиметричні протоколи розподілу ключів. Цифровий підпис. 1. Цифровий підпис та його властивості. Задачі, які розв'язує цифровий підпис. 2. Загальна класифікація типів протоколів розподілу ключів. Протокол Діффі-Геллмана. Основна література: [3]. Допоміжна література: [1]	**2,2**	2		0,2
Заняття 3/3	Протоколи узгодження ключів для конференц-зв'язку (групи користувачів). 1. Протоколи STS та MTI. 2. Протокол Діффі-Геллмана для трьох та більше сторін. Основна література: [4]. Допоміжна література: [4]	**2,5**		2	0,5

Заняття 3/4	Розв’язання завдань на дослідження властивостей криптографічної системи RSA. 1. Розв’язання задач зашифрування та розшифрування з використанням криптосистеми RSA. 2. Формування цифрового підпису повідомлень з використанням криптосистеми RSA. Основна література: [5]. Допоміжна література: [5]	**2,5**		2	0,5
Заняття 3/5	Розв’язання завдань на дослідження властивостей криптографічної системи Ель-Гамаля. 1. Розв’язання задач зашифрування та розшифрування з використанням криптосистеми Ель-Гамаля. 2. Формування цифрового підпису повідомлень з використанням криптосистеми Ель-Гамаля. Основна література: [5]. Допоміжна література: [5]	**2,5**		2	0,5
Тема 4	**Застосування криптографічних алгоритмів та протоколів для захисту інформації**	**10,9**	**4**	**4**	**2,9**
Заняття 4/1	Криптографічні ґеш-функції. Автентифікація об’єкту. Основні підходи до управління ключами. 1. Основні принципи побудови та призначення геш функцій. Криптографічні критерії ґеш-функції. 2. Фактори автентифікації. 3. Роль та місце управління ключами в системах криптографічного захисту інформації. Основна література: [3, 7] Допоміжна література: [4]	**2,2**	2		0,2
Заняття 4/2	Побудова, аналіз стійкості та застосування криптографічних геш-функцій. 1. Принципи побудови, функціонування, властивості геш-функцій сімейств MD та SHA. 2. Принципи побудови, функціонування, властивості ДСТУ 7564:2014. Основна література: [4, 7] Допоміжна література: [5]	**2,5**		2	0,5
Заняття 4/3	Модульна контрольна робота	**4**		2	2
Заняття 4/4	Перспективні напрями розвитку криптографії 1. Принципи побудови та функціонування систем шифрування, що побудовані на основі еліптичних кривих. 2. Постквантова криптографія. 3. Квантово-криптографічні протоколи. Основна література: [3]. Допоміжна література: [6]	**2,2**	2		0,2
Розрахункова робота		**6**			**6**
Залік		**8**		**2**	**6**
Всього годин		**60**	**20**	**20**	**20**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до заліку.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СРК
1	Тема 1. Математичні основи криптографії. 1. Розв'язання задач на використання класичних історичних алгоритмів шифрування. 2. Теоретико-інформаційна стійкість шифрів. 3. Розв'язання задач на криптоаналіз шифру простої заміни. 4. Шифр звичайного та багаторазового накладання двійкових гам. 5. Розв'язання задач на дослідження властивостей шифрів гамування. Основна література [1 – 5].	1,6
2	Тема 2. Принципи побудови та аналізу симетричних криптографічних систем. 1. Синхронізація потокових криптосистем. Принципи побудови потокових криптосистем. 2. Розв'язання задач на дослідження основних властивостей лінійних регістрів зсуву. 3. Потокові шифри. 4. Схема Фейстеля. Шифр DES. 5. Основні режими роботи блокових шифрів. 6. Алгоритм Rijndael. 7. Обмін ключами в симетричних криптосистемах. Основна література [1, 2, 3, 5, 6, 8].	1,6
3	Тема 3. Принципи побудови та аналізу асиметричних криптографічних систем. 1. Поняття односторонньої функції. 2. Криптографія з відкритим ключем. Відмінності від симетричної криптографії. 3. Задачі факторизації та дискретного логарифмування. 4. Поняття геш-функції. Сімейства MD та SHA. 5. Розв'язування задач на застосування криптосистем RSA та Ель-Гамаля. Основна література [3 – 5].	1,9
4	Тема 4. Застосування криптографічних алгоритмів та протоколів для захисту інформації. 1. Функції ґешування. 2. Схеми цифрового підпису на еліптичних кривих (Загальні положення; Процедура генерації ключів; Процедура підпису та перевірки). 3. Протоколи з нульовим розголошенням. 4. Поняття еліптичних кривих. 5. Національний стандарт ДСТУ 4145. 6. Стандарт функції гешування "Купина" ДСТУ 7564:2014. Основна література [3, 4, 7].	2,9
5	Розрахункова робота	6
6	Залік	6

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила захисту практичних робіт: в кожній практичній роботі має бути виконана практична частина та оформлений звіт, робота має бути захищена шляхом демонстрації практичної частини з поясненнями та відповіді на питання викладача.

Правила призначення заохочувальних та штрафних балів зазначені в РСО.

Політика дедлайнів та перескладань визначаються загальною політикою Інституту.

Політика академічної доброчесності: практичні роботи, що містять ознаки списування не приймаються і мають бути переробленими, а ті, що містять ознаки сторонньої допомоги при їх виконанні – також мають бути переробленими якщо курсант не надає вичерпних пояснень стосовно способу їх вирішення.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп,

проведення навчальних занять з даної навчальної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальні матеріали та ресурси, зазначені у розділі 4 цього силабусу є відкритими, не містять відомостей з обмеженим доступом і можуть бути оприлюднені з використанням технологій дистанційного навчання, а сам силабус не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання курсантів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів (студентів) в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтинг курсанта з кредитного модуля “Основи криптографії” визначається балами за роботу на:

1) лекціях
2) практичних заняттях.

При цьому враховуються заохочувальні (зі знаком “плюс”) та штрафні (зі знаком “мінус”) бали.

Система рейтингових (вагових) балів і критерії оцінювання

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою
Рейтингові бали, RD Оцінка за університетською шкалою

Кількість балів	оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше ніж 60	Незадовільно

1. Рейтинг курсанта з навчальної дисципліни “Основи криптографії” визначається балами за:

1) Індивідуальне завдання – розрахункова робота (максимальна кількість рейтингових балів: 1×25=25);

2) 2 усних опитувань, кожен з яких оцінюється у 5 балів (максимальна кількість рейтингових балів: 2×5=10);

3) 4 експрес-контролів, кожен з яких оцінюється у 10 балів (максимальна кількість рейтингових балів: 4×10=40);

4) модульної контрольної роботи (максимальна кількість рейтингових балів: 1×25=25).

При цьому враховуються заохочувальні (зі знаком “плюс”) та штрафні (зі знаком “мінус”) бали.

2. Критерії нарахування балів

2.1. Модульна контрольна робота.

– “відмінно”, повна відповідь (не менше 90% потрібної інформації) – 22-25 балів;
– “добре”, достатньо повна відповідь на задачу (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 19-21 балів;

– “задовільно”, завдання виконані з помилками та незначні помилки – 1-18 балів;
– “незадовільно”, не відповідає вимогам до “задовільно”– 0 балів.

2.2. Експрес-контроль.

–“відмінно”, виконані всі вимоги до роботи – 9-10 балів;
–“добре”, виконані майже всі вимоги до роботи, або є несуттєві помилки – 6-8 бали;
–“задовільно”, є недоліки щодо виконання вимог до роботи і певні помилки – 1-5 бали;
–“незадовільно”, не відповідає вимогам до “задовільно”– 0 балів.

2.3. Розрахункова робота.

– “відмінно”, повна відповідь (не менше 90% потрібної інформації) – 22-25 балів;
– “добре”, достатньо повна відповідь на задачу (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 19-21 балів;
– “задовільно”, завдання виконані з помилками та незначні помилки – 1-18 балів;
– “незадовільно”, не відповідає вимогам до “задовільно”– 0 балів.

Залікова контрольна робота оцінюється з 100 балів за такими критеріями:

– “відмінно”, повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 90-100 балів;

– “добре”, достатньо повна відповідь (не менше 75% потрібної інформації, або незначні неточності), що виконана згідно з вимогами до рівня умінь – 75-89 балів;

– “задовільно”, неповна відповідь (не менше 60% потрібної інформації та деякі помилки), що виконана згідно з вимогами до стереотипного рівня – 60-74 балів;

– “незадовільно”, незадовільна відповідь – 0-59 балів.

Умовою атестації є отримання не менше 50% від кількості балів, яку курсант може отримати на час проведення атестації.

Умовою допуску до заліку є: виконання усіх видів робіт та завдань, що передбачені робочим навчальним планом на семестр з цього кредитного модуля.

Сума рейтингових балів, отриманих курсантом протягом семестру, переводиться до підсумкової оцінки згідно з таблицею. Якщо сума балів ***менша за 60***, курсант виконує залікову контрольну роботу.

Курсант, який набрав протягом семестру необхідну кількість балів (***RD≥60***), отримує залікову оцінку (залік) так званим «автоматом» відповідно до набраного рейтингу. В такому разі до заліково-екзаменаційної відомості вносяться бали *RD* та відповідні оцінки.

Курсант, який у семестрі отримав більше 60 балів, може взяти участь у заліковій контрольній роботі з метою підвищення оцінки. У цьому разі бали, отримані ним на заліковій контрольній роботі, є остаточними.

Якщо оцінка за залікову контрольну роботу більша ніж за рейтингом, курсант отримує оцінку за результатами залікової контрольної роботи.

Якщо оцінка за залікову контрольну роботу менша, ніж за рейтингом, викладач застосовує жорстку РСО – попередній рейтинг курсанта з кредитного модуля скасовується і він отримує оцінку з урахуванням результатів залікової контрольної роботи.

9. Додаткова інформація з навчальної дисципліни

Питання для підготовки до залікової контрольної роботи

1. Цілі, послуги та механізми інформаційної безпеки.
2. Бінарні операції над цілими числами. Алгоритм ділення цілих чисел та вимоги до нього.
3. Теорія подільності цілих чисел та її чотири властивості.
4. Означення НСД двох цілих чисел, приклади.
5. Алгоритм Евкліда.
6. Операції за модулем.
7. Розширений алгоритм Евкліда.
8. Означення простих, складених та взаємно простих чисел.
9. Мала теорема Ферма та її застосування.
10. Теорема Ойлера та її застосування.
11. Алгебраїчні структури «група», «кільце» і «поле» та їх властивості.

12. Ідея симетричного шифрування. Принцип Керкгофса.
13. Основи криптоаналізу.
14. Шифри Бофора, Вернама та Віженера.
15. Блокові та потокові шифри.
16. Загальна класифікація шифрів.
17. Операції у сучасних блокових шифрах.
18. Регістри зсуву зі зворотним зв’язком.
19. Блоковий шифр DES.
20. Аналіз безпеки DES (2 DES та 3 DES).
21. Блоковий шифр AES.
22. Загальні положення та структура алгоритму ДСТУ ГОСТ 28147:2009.
23. Загальні положення ДСТУ ГОСТ 7624:2014.
24. Загальні положення ДСТУ ГОСТ 7564:2014.
25. Загальні положення ДСТУ ГОСТ 8845:2019.
26. Режими роботи блокових шифрів.
27. Шифр RC4.
28. Шифр A5/1.
29. Криптографічна система RSA.
30. Криптографічна система Ель-Гамаля.
31. Поняття ґеш-функції.
32. Поняття цифрового підпису.
33. Поняття автентифікації.
34. Основи управління ключами.
35. Методи розподілу відкритих ключів. Протокол узгодження ключів Діффі-Гелмана.