НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МАТЕМАТИЧНИХ МАШИН І СИСТЕМ

ЗАТВЕРДЖЕНО
рішенням вченої ради
ІПММС НАН України
від « 03 » серпня 2022 року
протокол № 7

РОБОЧА НАВЧАЛЬНА ПРОГРАМА
ДИСЦИПЛІНИ

«МЕТОДИ І МОДЕЛІ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ БЕЗПЕКИ»

Третій освітньо-науковий
рівень вищої освіти – доктор філософії

Спеціальність – 122 Комп'ютерні науки

Київ 2022

І. ЗАГАЛЬНІ ВІДОМОСТІ

Актуальність дослідження теоретичних та прикладних проблем забезпечення комп'ютерної безпеки обумовлена широким застосуванням інформаційних технологій у критичній інфраструктурі та зростанням сили та частоти реалізації загроз кібербезпеки. Сучасний дослідник комп'ютерних технологій повинен обґрунтовано обирати принципи їх реалізації з урахуванням необхідності забезпечення надійного захисту інформаційних ресурсів. Це обумовлює мету викладання дисципліни.

Метою дисципліни «Методи і моделі забезпечення комп'ютерної безпеки» є отримання аспірантами теоретичних знань та практичних навичок, що стосуються базових методів захисту інформації, їх стійкості, математичних моделей відповідних процесів.

ІІ. РОЗПОДІЛ УЧБОВОГО ЧАСУ

Семестр	Семестрова атестація	Всього	Розподіл за семестрами та видами занять				
			Лекції	Практичні заняття	Семінари	Лаб. роботи	Самостійна робота
3	Екзамен	60	50	-	-	-	10
Кількість кредитів		2					

Перелік основних компетенції та результатів, що мають бути набути протягом навчання наведено в таблиці 1.

Таблиця 1

Обов'язкові компетентності		**Результати навчання**
Загальні компетентності	**Спеціальні (фахові) компетентності**	
ЗК01. Здатність до абстрактного мислення, аналізу та синтезу. **ЗК02**. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК04.** Здатність розв'язувати комплексні проблеми комп'ютерних наук на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності	**СК01.** Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей. **СК02.** Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності. **СК03.** Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень. **СК05.** Здатність здійснювати науково-педагогічну діяльність у вищій освіті у сфері комп'ютерних наук **СК06**. Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій	**РН01**. Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій. **РН03**. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. **РН04**. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямах. **РН05.** Планувати і виконувати

		експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. **РН08**. Визначати актуальні наукові та практичні проблеми у сфері комп'ютерних наук, глибоко розуміти загальні принципи та методи комп'ютерних наук, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері комп'ютерних наук та у викладацькій практиці

ІІІ. ЦІЛІ ТА ЗАДАЧІ ДИСЦИПЛІНИ

Згідно з вимогами освітньо-професійної програми аспіранти повинні:

розуміти:

- математичну та фізичну суть утворення каналів впливу/ витоку інформації;
- різницю між антропогенними, техногенними та природними загрозами кібербезпеки;
- сутність комплексного підходу щодо захисту інформації в комп'ютерних системах.

володіти:

- методами аналізу технологій криптографічного та технічного захисту інформації;
- методами побудови адекватних моделей загроз і моделей порушників безпеки;
- методами раціонального вибору архітектури системи захисту;
- методами управління ризиками;
- статистичними методами досліджень криптосистем та їх компонентів;
- алгебраїчними методами досліджень криптосистем та їх компонентів.

вміти:

- реалізовувати ефективні процедури побудови комплексних систем захисту;
- використовувати апарат комбінаторного аналізу, теорії ймовірностей і математичної статистики для оцінки ступеню виконання завдань із захисту;
- будувати на основі фізичних випадкових процесів генератори паролів, ключів та інших параметрів систем безпеки.

IV. ТЕМАТИЧНИЙ ПЛАН

IV.1. ***Розподіл учбового часу по темах***

Назва розділів, тем	Розподіл за семестрами та видами занять						
	Всього годин	Лекції, годин	Практ. заняття годин	Семінари, годин	Лаб. роботи, годин,	Комп. практ, годин	Самостійна робота годин
1	2	3	4	5	6	7	8
Семестр 1							
Модуль 1. Базові поняття теорії і практики захисту інформації	14	10					4
Тема 1. **Характеристики об'єктів захисту** Характеристика інформації, її властивості, що підлягають захисту, моделі відкритих повідомлень. Класифікація комп'ютерних систем. Принципи розвідки. Канали витоку та впливу на інформацію. Модель системи секретного зв'язку по Шеннону. Екологія інформаційного простору, інформаційна безпека, комп'ютерна безпека, мережна безпека, кібербезпека. Рівні безпеки.	6	4					2
Тема 2. **Моделі загроз та моделі порушника** Класифікація загроз безпеки комп'ютерних систем. Характеристика антропогенних, техногенних та природних загроз.	6	4					2
Тема 3. **Оцінка ризиків** Залежності елементів захисту та залежності у керуванні ризиками. Цінності активів та вразливості стосовно типів загроз.	2	2					
Модуль2. Політика безпеки та моделі безпеки	14	10					4
Тема 4. **Основи побудови моделей при проектуванні систем захисту**	2	2					
Тема 5. **Політика безпеки** Поняття політики безпеки. Поняття доступу та монітора безпеки. Розробка і реалізація політики безпеки. Домени безпеки.	6	4					2
Тема 6. **Модель безпеки** Модель матриці доступу. Безпека системи. Модель безпеки Белла-Лападула. Модель безпеки інформаційних потоків. Комбінована матрично-мандатна модель безпеки.	6	4					2

Модуль 3. Комп'ютерна криптографія	20	20					
Тема 7. **Основні поняття і задачі криптології** Предмет, мета і завдання криптографії і криптоаналізу. Базові поняття у галузі криптографічного захисту. Рівняння криптографічного перетворення у загальному вигляді, сутність симетричних та асиметричних шифрів. Практичні вимоги до криптосистем. Класифікація шифрів: блокові та потокові шифри, попереднє шифрування та лінійне засекречування. Елементарні шифри: простої заміни, перестановки, Хілла, Вернама, Віжинера та їх властивості. Методи побудови складних шифрів, операції з шифрами по Шеннону. Теорема Маркова. Приклади комбінацій елементарних шифрів в стандартах криптографічних перетворень.	4	4					
Тема 8. **Моделі загроз безпеки криптосистем** Етапи життєвого циклу засобів КЗІ та їх характеристика. Загальна схема засобу КЗІ. Модель Шеннона. Принцип Кекхофса, види атак на криптосистеми. Класифікація засобів КЗІ по рівнях безпеки. Вимоги з безпеки для криптографічних модулів в стандарті ДСТУ ISO/IEC 19790:2015. Методи побудови шифрів на основі рекурентних схем (РС). Характеристика основних елементів РС та їх властивості: бульові функції. комутатори, регістри зсуву. Принципи побудови блокових шифрів (криптоалгоритмів) у стандартах ДСТУ ГОСТ 28147:2009, ДСТУ 7624-2014, AES. Характеристика режимів роботи блокових алгоритмів ECB, CBC, CFB, OFB. Принципи розробки, досліджень та сертифікації криптосистем.	4	4					
Тема 9. **Методи КЗІ від маніпуляцій у комп'ютерних системах** Модель загроз. Принципи побудови та застосування функцій хешування. Поняття імітостійкості повідомлень. Формування та застосування кодів автентифікації повідомлень (MAC) для контролю цілісності. Процедури електронного цифрового	4	4					

підпису (ЕЦП). Механізми формування та перевіряння ЕЦП на прикладі алгоритмів RSA та Ель Гамалю. Криптографія в операційних системах Windows. Поняття про ЕЦП на еліптичних кривих.							
Тема 10. **Криптографічні протоколи** Застосування криптографічних протоколів в системах захисту інформації. Методи автентифікації користувачів за допомогою симетричних та асиметричних криптосистем. Стандарти захищених протоколів в мережі Інтернет. Управління ключами. Етапи життєвого циклу криптографічних ключів. Особливості генерації та тестування ключової інформації. Генератори псевдовипадкових чисел. Поняття про генерацію простих чисел для асиметричних криптосистем.	4	4					
Тема 11. **Архітектура захищених мереж** Методи побудови повно зв'язаних мереж. Застосування лінійного та попереднього шифрування. Особливості криптографічного захисту в мережах мобільного зв'язку Характеристика мереж транкінгового та стільникового зв'язку. Принципи побудови та властивості криптографічних алгоритмів A5/1, A5/2. Архітектура систем ЕЦП. Центр сертифікації ключів. Стандарт сертифікату відкритого ключу X.509.	4	4					
Модуль 4. Методологія побудови захищених систем	12	10					
Тема 12. **Метрики в оцінці безпеки** Критерії безпеки що визначені НД ТЗІ.	6	4					2
Тема 13**. Європейські критерії безпеки інформаційних технологій**	2	2					
Тема 14**. Технологія побудови систем захисту**	4	4					
Всього за 1 семестр	60	50					10

V. ПОТОЧНИЙ ТА ПІДСУМКОВИЙ КОНТРОЛЬ

Поточний контроль здійснюється під час проведення лекцій та практичних занять.

Підсумковий контроль – це оцінювання засвоєння студентами всього теоретичного матеріалу та рівня практичної підготовки з навчальної дисципліни.

Підсумкова оцінка виставляється за результатами поточного контролю за шкалою оцінювання, наведеною в таблиці 2.

Таблиця 2

Оцінка (за національною шкалою)	**Бали**
Атестований з оцінкою "відмінно"	91-100
Атестований з оцінкою "добре"	76-90
Атестований з оцінкою "задовільно"	60-75
Не атестований з оцінкою "незадовільно"	26-59
Не атестований з оцінкою "н/а"	0-25

Формою підсумкового контролю успішності навчання аспірантів є **екзамен.**

VI. ЗАСОБИ ДЛЯ ПРОВЕДЕННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Модульний контроль 1, 2

1. Комплексна система захисту інформації це:
а. технічний та криптографічний захист, нормативні та організаційні заходи;
б. обстеження, зашумлення та програмно-апаратні заходи;
в. нормативні та організаційні заходи, обстеження та заземлення.
2. Технічні канали витоку інформації це:
а. крадіжки, недбалість, порушення правил користування системами антивірусного захисту;
б. втручання в роботу систем електроживлення;
в. акустика, оптика, електромагнітні випромінювання, кола живлення.
3. Властивості інформації, що підлягають захисту.
а. достовірність, недоступність, цілісність;
б. таємність, недоступність, цілісність;

в. цілісність, конфіденційність, доступність.

4. Пасивні методи захисту від витоку інформації за рахунок ПЕМВН це:

а. екранування, зниження потужності небезпечних електричних сигналів та їх фільтрація;.

б. зашумлення, екранування та застосування антивірусного захисту;

в. заземлення, зашумлення, звукопоглинання

5. Термін «об'єкт інформаційної діяльності» включає:

а. транспортні засоби та стаціонарні об'єкти, де циркулює інформація, яка захищається;

б. транспортні засоби для перевезення засобів інформаційної безпеки;

в. стаціонарні об'єкти що призначені для розміщення засобів масової інформації.

6. Законодавство поділяє інформацію з обмеженим доступом на:

а. конфіденційну, особисту, державну таємницю

б. службову, таємницю, конфіденційну;

в. персональні дані, статистичні дані, екологічну інформацію.

7. Залежно від джерела походження загрози поділяють на:

а. природні загрози та іноземне втручання,

б. електричні, оптичні, акустичні;

в. людський фактор, природні та техногенні загрози.

8. Модель загроз безпеки інформації це:

а. опис потенційних загроз що мають бути враховані під час побудови КСЗІ;

б. опис можливостей порушника;

в. таблиця нереальних загроз

9. Модель порушника безпеки інформації враховує:

а. його технічні можливості, умови доступу до ресурсів системи, наявність спільників та зброї;

б. особливості проведення інвентаризації технічних засобів обробки інформації;

с. його рівень знань, технічні можливості, час та місце дії.

10. Блокування акустичних каналів витоку інформації забезпечується завдяки:

а. звукопоглинанню, зашумленню, спеціальним архітектурним рішенням;

б. звукопоглинанню, екрануванню, зашумленню;

в. зашумленню, екрануванню, зменшенню розміру об'єкту інформаційної діяльності.

11. Несанкціонований доступ в автоматизованих системах це:

а. доступ до ресурсів системи з використанням штатних засобів системи;

б. порушення норм захисту від підслуховування у мережних з'єднаннях;

в. нештатна ситуація у випадку відключення електроживлення.

12. Етапи створення КСЗІ, зокрема, включають:

а. розробку моделі порушника інформаційної безпеки, ліквідацію вірусів, випробування КСЗІ;

б. обстеження об'єкту, формування моделі загроз інформаційної безпеки, випробування КСЗІ;

в. обстеження об'єкту, експертизу КСЗІ, блокування космічних каналів впливу на інформацію.

13. Шкідливі програми це:

а. «хробаки», «трояни», «логічні бомби»;

б. «трояни», «логічні бомби», ігрові програми;

в. недокументовані прикладні програми.

14. Методи розмежування доступу в АС

а. забезпечують ідентифікацію користувачів та блокують спроби несанкціонованого доступу;

б. реалізують автентифікацію та забезпечують антивірусний захист;

в. надають можливість доступу до критичних ресурсів всім користувачам системи.

15. Задачі заходів адміністративного рівня забезпечення ІБ

а. інсталяція та обслуговування засобів захисту інформації

б. створення програмного забезпечення захисту інформації;

в. формування організаційної структури захисту інформації та затвердження керівних документів.

Модульний контроль 3,4

Варіант 1	Варіант 2
1. Криптографія вивчає: **А**) методи захисту інформації шляхом її стискання; **Б**) технології блокування технічних каналів витоку інформації; **В**) методи захисту інформації шляхом її перетворень за допомогою секретних параметрів - ключів.	**1. Криптоаналіз досліджує:** **А**) можливість розкриття шифрів без знання секретного ключу; **Б**) умови захисту інформації шляхом блокування каналів її витоку; **В**) контроль цілісності інформації за допомогою її асиметричних перетворень.
2. Криптоперетворення слугують вирішенню наступних задач: **А**) забезпечення конфіденційності інформації та перевірка її авторства; **Б**) забезпечення доступності інформації та контроль її цілісності; **В**) автентифікація суб'єктів доступу до інформації та контроль її якості.	**2. Об'єктами досліджень у криптографії, зокрема, є:** **А**) методи відновлення втрачених даних; **Б**) схеми побудови засобів стискання даних; **В**) системи генерації та розподілу ключів.
3. Ключі зашифрування та розшифрування у симетричних криптосистемах: **А**) не співпадають і не можуть бути обчислені один з іншого; **Б**) збігаються або один з іншого може бути легко обчислений; **В**) співпадають, але один з них відкритий, а інший секретний.	**3. Симетричні криптосистеми переважно використовуються для:** **А**) перевіряння цілісності та доступності повідомлень; **Б**) шифрування довгих повідомлень та генерації ключів; **В**) підтвердження авторства даних та визначення їх цінності.
4. Асиметричні криптосистеми переважно використовуються для: **А**) шифрування даних великого обсягу; **Б**) для реалізації виду шифрування «цифровий конверт» та «цифровий підпис»; **В**) перевіряння цілісності інформації та її доступності.	**4. В асиметричному шифрі ключі зашифрування і розшифрування:** **А**) не співпадають, а обчислення одного з другого є складною практично нерозв'язною задачею; **Б**) збігаються, але один з них відкритий, а інший секретний; **В**) співпадають або один з іншого може бути просто обчислений.
5. Дешифрування – це: **А**) зворотна до розшифрування процедура; **Б**) метод відновлення відкритого тексту без знання ключа;	**5. Зашифрування – це:** **А**) зворотна до дешифрування процедура; **Б**) процедура перетворення шифрованого повідомлення у відкрите;

В) процес перетворення відкритого тексту у шифрований за допомогою ключа.	**В**) метод розкриття відкритого тексту з використанням ключа.
6. Теоретично стійка криптографічна система: **А)** виключає можливість її розкриття шляхом повного перебору ключів **Б)** може бути розкритою тільки за допомогою суперкомп'ютерів; **В)** не може бути застосована для захисту інформації у комп'ютерних мережах.	**6. Криптосистема вважається практично стійкою:** **А)** якщо довжина її ключу дорівнює довжині шифрованого тексту; **Б)** якщо за допомогою найшвидшого сучасного суперкомп'ютеру ключ не буде знайдений ніколи; **В)** за допомогою жодного відомого методу криптоаналізу за визначений час не можливо знайти її ключ.
7. Збільшення довжини бітового ключу в криптосистемі на 4 біта призведе до збільшення різних кількості ключів: **А**) в 8 разів; **Б**) на 8; **В**) в 16 разів.	**7. Зменшення довжини бітового ключу в криптосистемі на 3 біта призведе до зменшення різних кількості ключів:** **А)** на 6; **Б)** в 8 разів; **В)** в 3 рази.
8. Хеш-функція: **А)** дозволяє сформувати короткий дайжест повідомлення; **Б)** контролює цілісність даних; **В)** забезпечує конфіденційність.	**8. MAC-код (код автентифікації) дозволяє контролювати:** **А)** конфіденційність інформації; **Б)** цілісність інформації; **В)** оперативність інформації.
9. У разі блокового шифрування даних забезпечується: **А**) зменшення довжини повідомлення; **Б**) шифрування «відрізків» відкритого тексту довжиною по декілька символів кожен; **В**) контроль достовірності даних.	**9. В випадку попереднього шифрування:** **А**) передача даних в канал і шифрування здійснюються одночасно; **Б**) одночасно цифровий підпис ніколи не використовуються; **В**) передача інформації в канал і шифрування рознесені в часі.
10. Криптосистема - це: **А)** математичний опис алгоритму; **Б)** організаційно-технічна система, що включає її обслуговуючий персонал; **В)** сукупність засобу КЗІ та необхідної документації	**10. Програмний засіб КЗІ – це:** **А)** програма що реалізує шифрування у середовищі комп'ютера **Б)** засіб КЗІ що обслуговується за певною програмою; **В)** засіб що електричне підключений до комп'ютера.
11. Стандарти блокового шифрування: **А**) можуть застосовувати схему Файстеля; **Б**) не реалізують режим «кодова книга»; **В**) забезпечують достовірність інформації	**11. Шифр Вернама забезпечує:** **А)** заміну чергового символу відкритого тексту за допомогою ключу що має дві стрічки; **Б)** заміну символу відкритого тексту залежно від чергового біту ключа; **В**) зміну порядку слідування символів в шифротексті.
12. Для захисту службової інформації використовують засоби КЗІ: **А)** такі що мають сертифікат; **Б)** допущені до експлуатації;	**12. Для захисту державної таємниці використовують засоби КЗІ:** **А)** сертифіковані в системі УкрСЕПРО; **Б)** мають атестат відповідності;

В) такі що реалізують світові стандарти.	**В)** допущені до експлуатації.
13. Процедура експертизи у галузі КЗІ передбачає перевірку: **А)** спроможності суб'єктів господарської діяльності виконати роботи у галузі КЗІ; **Б)** відповідності засобів КЗІ вимогам нормативних документів; **В)** рівня безпеки обладнання для виготовлення засобів КЗІ.	**13. Процедура ліцензування у галузі КЗІ включає:** **А)** подачу суб'єктом господарської діяльності відомостей про наявність спеціалістів у галузі КЗІ **Б)** оцінку відповідності наявного обладнання вимогам стандартів; **В)** створення фінансового фонду для страхування можливих збитків.
14. Для акредитації центр сертифікації ключів (ЦСК) повинен: **А)** мати надійні засоби ЕЦП; **Б)** мати шифровані канали зв'язку; **В)** вести реєстр усіх доступних ЦСК.	**14. Центральний засвідчувальний орган (ЦЗО) підпорядкований:** **А)** Міністерству транспорту та зв'язку; **Б)** Адміністрації Держспецзв'язку; **В)** Міністерству юстиції. .
15. Центральний засвідчувальний орган (ЦЗО): **А)** генерує ключі підписувачам; **Б)** формує ЕЦП органам державної влади; **В)** акредитує ЦСК	**15. Центр сертифікації ключів (ЦСК) надає послуги:** **А)** акредитації засвідчувальних центрів; **Б)** генерації довготермінових ключів; **В)** генерації пар ключів електронного цифрового підпису.
16. Засвідчувальний центр (ЗЦ): **А)** створюється для державних органів; **Б)** формує сертифікати секретних ключів; **В)** генерує головні (мастер) ключі	**16. Послуги електронного цифрового підпису (ЕЦП) державним органам надають:** **А)** Тільки ЦЗО; **Б)** ЦЗО та акредитовані ЦСК; **В)** Тільки акредитовані ЦСК.
17. Безпека криптосистеми RSA побудована на складності практичного розв'язку задачі: **А**) знаходження логарифму великих чисел у кінцевій множині; **Б**) знаходження суми двох надвеликих чисел; **В**) розкладання великих чисел на прості множники.	**17. Стійкість криптосистеми Діффі-Хеллмана базується на складності розв'язку задачі:** **А**) розкладання великих чисел на прості множники; **Б**) знаходження логарифму великих чисел у кінцевій множині; **В**) обчислення квадратичного кореню з великого числа.
18. Клас безпеки засобу криптографічного захисту інформації встановлюється на рівні Б2, якщо: **А**) використовується дворівнева система розмежування доступу; **Б**) додатково до інших рівнів безпеки забезпечене блокування побічних каналів витоку; **В**) безпека засобу базується тільки на стійкості криптоалгоритму та правильності його реалізації.	**18. Клас безпеки засобу криптографічного захисту інформації встановлюється на рівні В3, якщо:** **А**) безпека засобу базується тільки на стійкості криптоалгоритму та правильності його реалізації; **Б**) забезпечується надійність захисту в сучасних науково-технічних умовах; **В**) використовується трирівнева система розмежування доступу.
19. Перевагою виду шифрування «лінія	**19. Вид шифрування «із кінця в кінець»:**

за лінією» є: **А**) суттєва економія необхідних ключів; **Б**) підвищена безпека інформації на вузлах комутації; **В**) можливість застосування для побудови мережі різних типів засобів КЗІ.	**А**) виключає витік інформації на вузлах комутації; **Б**) забезпечує можливість застосування різних за алгоритмом засобів КЗІ; **В**) виключає необхідність зміни ключів.

20. Алгоритм шифрування А5/1 у системі мобільного стільникового зв'язку стандарту GSM забезпечує захист: **А)** тільки радіоканалу; **Б)** «із кінця в кінець»; **В)** залежно від налаштувань.	**20. Перевагою систем мобільного транкінгового зв'язку є:** **А)** можливість одночасного виклику кількох абонентів; **Б)** забезпечення конфіденціності радіоканалу без шифрування; **В)** Нічого з наведеного

Еталони (зразки) відповідей до завдань РКР

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	В	А	Б	Б	Б	А	В	А	Б	В	А	Б	Б	А	В	А	В	Б	В	А
2	А	В	Б	А	Б	В	Б	Б	А	А	Б	В	А	В	В	В	Б	А	Б	А

Творчі завдання

Варіант 1.

1. Наведіть приклад шифру простої заміни в алфавіті A={A,B,C,D,E}.
2. Наведіть свій приклад шифру перестановки для повідомлення української мови з довжиною ключу 4.

Варіант 2.

1. Наведіть приклад шифру простої заміни в алфавіті A={1,2,3,4,5,6,7}
2. Наведіть свій приклад шифру перестановки для повідомлення української мови з довжиною ключу 5.

VII. ПЕРЕЛІК ЕКЗАМЕНАЦІЙНИХ ПИТАНЬ

1. Характеристика понять: екологія інформаційного простору, інформаційна безпека, комп'ютерна безпека, мережна безпека, кібербезпека.

2. Методи та наслідки несанкціонованого втручання в роботу комп'ютерних систем. Канали витоку та впливу на інформацію.

3. Поняття про моделі відкритих повідомлень. Властивості інформації, що підлягають захисту.
4. Модель загроз безпеки інформації та модель порушника безпеки інформації.
5. Класифікація загроз безпеки комп'ютерних систем, характеристика антропогенних, техногенних та природних загроз.
6. Загальна характеристика методів технічного захисту інформації в комп'ютерних системах.
7. Сутність та переваги матричного та мандатного методів розмежування доступу в комп'ютерних системах.
8. Методи виявлення шкідливих кодів.
9. Заходи протидії атакам типу «відмова в обслуговуванні» (DOS).
10. Мета створення та зміст політики інформаційної безпеки організації.
11. Комплексна система захисту інформації, її складові та етапи створення.
12. Сутність та складові багаторівневої системи захисту в інформаційній системі.
13. Процесний підхід до побудови системи управління інформаційною безпекою (СУІБ). Управління ризиками. Процесна модель СУІБ.
14. Характеристика процедур сертифікації систем безпеки та їх оцінки за методом «проникнення» (pentest).
15. Основні поняття комп'ютерної криптографії: зашифрування та розшифрування, дешифрування.
16. Сутність і завдання криптографічного захисту інформації (КЗІ) в комп'ютерних системах.
17. Рівняння зашифрування та розшифрування у загальному вигляді та їх параметри.
18. Модель секретного зв'язку по Шеннону, види атак на криптосистеми. Принцип Керкхофса щодо безпеки криптосистем.
19. Операції з шифрами по Шеннону. Елементарні шифри та їх властивості.
20. Теоретична та практична стійкість криптографічних перетворень, абсолютно стійкий шифр Вернама.
21. Класифікація криптосистем: симетричні та асиметричні, блокові та потокові.
22. Застосування асиметричних криптосистем в комп'ютерних системах: процедури електронного цифрового підпису, цифрового конверту, розподілу ключів.
23. Стадії життєвого циклу криптографічних ключів, вимоги до двійкових ключів криптосистем.
24. Основні складові безпеки застосування засобів КЗІ. Приховані канали витоку критичної інформації про засоби КЗІ.
25. Характеристика засобів криптографічного захисту інформації залежно від їхньої реалізації, класифікація засобів КЗІ за рівнями безпеки.
26. Хеш функції та їх властивості. Застосування хеш функцій в комп'ютерних системах.
27. Методологія побудови блокчейн систем.
28. Призначення коду автентифікації повідомлень MAC. Формування MAC за допомогою алгоритму блокового алгоритму шифрування.
29. Побудова асиметричних криптосистем на основі складності розв'язку задач факторизації чисел (RSA) та логарифмування в кінцевому полі. Застосування еліптичних кривих в криптографії.

30. Поняття криптографічного протоколу. Алгоритм Диффі-Хеллманна формування спільного ключу.
31. Криптографічні перетворення в середовищі ОС WINDOWS. Поняття сильних паролів.
32. Нормативна правова база забезпечення захисту інформації та кібербезпеки.

VIII. НАВЧАЛЬНО-МЕТОДИЧНА ЛІТЕРАТУРА

Основна література

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник/ - Вінниця: ВНТУ, 2011. -199с.
2. Голев Д.В. Інформаційна безпека інформаційно – комунікаційних систем. Навч. Посібник / Г. Кононовича. / Д.В. Голев, О.Ю. Русляченко, Ю.В. Бєлова, Д.С. Гончарук – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 184 с.
3. Мохор В.В., Богданов А.М., Килевой А.С. Наставления по кибербезопасности (ISO/IEC 27032:2012). - К.: Три-К. 2013.

Базова література

1. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія/ За заг. ред. д.т.н., професора Горбенка І.Д. – Харків: Вид. «Форт», 2015.
2. Ленков С.В., Перегудов Д.А., Хорошко В.А., Методы и средства защиты информации/ под. ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность, – 344 с.
3. Криптологія в тестах, задачах і прикладах: навч. посібник/ Т.В.Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомічова. – Д.: Національний гірничий університет, 2013, - 356с.
4. Mark Stamp, Richard M. Low. Applied cryptoanalysis: breaking ciphers in the real world. J.Wiley&Sons, Inc. Hoboken, New Jersey. 2007.

Допоміжна література

1 Математичні основи криптографії: навч. посібник/ Г.В. Кузнецов, В.В. Фомічов, С.О. Сушко, Л.Я. Фомічова. – Д.: Національний гірничий університет, 2004, — 391 с.
2. Математичні основи криптоаналізу: навч. посібник/ С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомічова, А.В. Корабльов. – Д.: Національний гірничий університет, 2010, — 465 с.
3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] - Львів, «Магнолія 2006», 2013. – 256 с.
4. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] - Львів, «Магнолія 2006», 2014. – 312 с.

Програму склав
д.т.н., доцент **ГУЛАК Г.М.**