Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

1. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства
1	История криптографии	*Контрольные вопросы. Контрольные задачи. Экзамен*
2	Основные понятия криптографии	*Контрольные задачи. Контрольные вопросы. Экзамен*
3	Криптография и прикладная математика	*Контрольные вопросы. Контрольные задачи. Экзамен*
4	Модели открытого текста	*Контрольные вопросы. Контрольные задачи. Экзамен*
5	Шифры перестановки и шифры замены	*Контрольные вопросы. Контрольные задачи. Экзамен*
6	Шифры гаммирования	*Контрольные вопросы. Контрольные задачи. Экзамен*
7	Требования к криптографическим преобразованиям и шифрсистемам	*Контрольные вопросы. Контрольные задачи. Экзамен*
8	Генерация псевдослучайных последовательностей	*Контрольные задачи. Контрольные вопросы. Экзамен*
9	Блочные шифры	*Контрольные вопросы. Контрольные задачи. Экзамен*
10	Системы шифрования с открытыми ключами	*Контрольные вопросы. Контрольные задачи. Экзамен*
11	Электронная цифровая подпись	*Контрольные вопросы. Контрольные задачи. Экзамен*
12	Методы проверки подлинности объекта коммуникации	*Контрольные вопросы. Контрольные задачи. Экзамен*
13	Функции хеширования	*Контрольные вопросы. Контрольные задачи. Экзамен*
14	Управление ключами	*Контрольные вопросы. Контрольные задачи. Экзамен*
15	Основы технологии инфраструктур открытых ключей	*Контрольные вопросы. Контрольные задачи. Экзамен*
16	Криптографическое обеспечения информационной безопасности в сети Internet	*Контрольные вопросы. Контрольные задачи. Экзамен*

17	Практические аспекты использования шифрсистем	*Контрольные вопросы. Контрольные задачи. Экзамен*
18	Нормативная база в области криптографической защиты информации	*Контрольные вопросы. Контрольные задачи. Экзамен*

2. Виды контроля по периодам обучения

2.1 Материалы для проведения текущего контроля:

Наименование оценочного средства (в соответствии с паспортом фонда оценочных средств) Контрольные вопросы. Контрольные задачи

Перечень контрольных вопросов:

- Алгебраическая модель шифра замены.
- Алгебраическая модель шифра перестановки.
- Алгебраическая модель шифра RSA.
- Вероятностная модель шифрования.
- Алгебраические модели открытого текста.
- Вероятностные модели открытого текста.
- Принципы построения криптографических алгоритмов блочных шифров.
- Криптографические параметры «перемешивающих» и «рассеивающих» блоков.
- Композиции шифров.
- Синтез шифров DES алгоритма.
- Принципы построения криптографических алгоритмов поточного шифрования.
- Линейные регистры сдвига.
- Характеристический многочлен линейного регистра сдвига
- Композиции линейных регистров сдвига.
- Вопросы организации сетей засекреченной связи. Ключевые системы.
- Криптографические хеш-функции.
- Криптографические протоколы.
- Протоколы идентификации.
- Таблица Виженера
- Криптографическая стойкость шифров.
- Шифр Виженера.
- Шифратор «Энигма»
- Шифратор «Хагелин»
- Математическая теория криптографии Клода Шеннона.
- Телефонные шифраторы.
- Стандарт шифрования данных (DES).
- Имитостойкость.
- Ключи, ключевая система, распределение ключей.
- Имитостойкость и помехоустойчивость шифров.
- Шифры перестановки и их свойства.
- Элементы криптоанализа шифров перестановки.
- Шифры замены и их свойства.
- Криптоанализ шифра простой замены.
- Шифры гаммирования.
- Криптоанализ шифра Виженера.

- Системы шифрования с открытыми ключами.
- Шифрсистема RSA.
- Электронная цифровая подпись.
- Цифровые подписи на основе шифрсистем с открытыми ключами
- Шифрование в телефонии.
- Скремблирование.
- Критерии распознавания открытого текста.
- Энтропия и избыточность языка.
- Расстояние единственности.
- Аппаратные реализации шифров.
- Программные реализации шифров.
- Методы получения случайных и псевдослучайных последовательностей.
- Функции хэширования и целостность данных.
- Протоколы распределения ключей.
- Частотные преобразования речевого сигнала.

Перечень контрольных задач:

Задача 1. Провести криптографический анализ засекреченного сообщения. Установить используемую систему шифрования. Дешифровать засекреченное сообщение.

Исходные данные: Шифртекст:

Э ъ л ф ш ы э ф п с ф а ш ы л э в д ш ф м е ы е з ф ъ е х щ т п ж ю к э ж п ы и ф о ж ф з п л ы х э и ю м п л л ф о п х
е ш т п х в ч ф м э э и ц ж п п г п ж п т в ы э ы ц ш в к к ф ж п л ф г ж ф о э п м м ц д ш п ж с е ы т п ж п л э м е ь ы э
д ш э ж ш ы п в ж е м е я ч м п а о х е м э з ф т х п л э м з э э ю х ф г э х ю и э г п м с ф а ш ы л п л е ы щ м е с п и ц
ж п г е г й п ч м п ш г п х ф ф к ы п и ц ъ е д л е ы э ы щ ш ф м е ы л х е ш т ж п д т п г е ф р ф м ф т х э н ж п п б э з
э е ж щ м п ф э ъ л ф ш ы э ф п т х п л ф с ф м м ц д м е г п м ф з ъ е г п м м ц й п и х е ъ п й ы х ф и п л е м э в д ш ф
м е ы е с ф м щ с ф ш в ы п о п в м л е х в п м ы е а м п п ы л ш ф д т п ш л в р е ф ы м ю ч м ц й х е ш т п х в ч ф м э
в й м п к щ я п т в ы щ ы е г э ы е а м п ш м ф ш г п ж щ г э й э и ж э ъ г э й э и х п ш е ф ы ш в г л п а ш г ю э т ф х ф
д п с э ы о х е м э з ю ш л п ф а т х п л э м з э э х ю и э г п м

Задача 2. Провести криптографический анализ и дешифрование засекреченного сообщения, полученного применением шифра Цезаря.

Исходные данные: Шифртекст:

х с й е т п а ь м р ж т н х о т р т с ж х ц ч у м п ж д п й о х д с и ф м в м ж р й ь д п х г ж т ж с ч ц ф й с с м й и й п д й
з м у ц д й з м у й ц с ч к й с е я п й р ч о д о е т з д ц й н ь д г х ц ф д с д м у ф м ж п й о д п й з т х ж т й н х п т к с т
н м м х о ч х с т н д и р м с м х ц ф д ц м ж с т н т ф з д с м л д ъ м й н л д и й ф к д п д й з т м х ж г л а х о п й т у д ц
ф т н х й х ц ф т н м к й с т н р т п т и т з т у ц т п й р й г у й ф ж я р д о ц т р ъ й л д ф г е я п т ж т и ж т ф м ц а ж т и
ж т ф ъ й у ф т з с д с с ч в р ч к й р о п й т у д ц ф ч ж т т е э й т с ф д х у т ф г к д п х г ж д п й о х д с и ф м м о д о у
т п с т ж п д х ц с я н щ т л г м с о д о р т с д ф щ б ц т ж х ж г л м х т х п д е т х ц а в й з т ж т н х о д у т и с г п т ж д
п й о х д с и ф м м с д с т з м ж х й с д х й п й с м й

Задача 3. Используя шифр Виженера зашифровать фразу: FINIS CORONAT OPUS с помощью ключевого слова VERBA.

Задача 4. Используя шифр Виженера расшифровать сообщение: A M E J S X S I P N V X F Q U N с помощью ключевого слова VERBA.

Задача 5. Используя шифр гаммирования зашифровать фразу: ALTER EGO с помощью случайной равновероятной гаммы UDLGOXTA

Задача 6. Используя шифр гаммирования расшифровать сообщение: UOEKFBZO с помощью случайной равновероятной гаммы UDLGOXTA

Задача 7. Используя шифр Цезаря зашифровать фразу: THE POETRY IS NEVER DEAD с помощью ключа D

Задача 8. Используя шифр Цезаря расшифровать сообщение: WKH SRHWUB LV QHYHU GHDG. Ключ неизвестен.

Задача 9. Используя шифр Сцитала зашифровать фразу: МУЗА СКАЖИ МНЕ О ТОМ МНОГООПЫТНОМ МУЖЕ КОТОРЫЙ при помощи цилиндра с длинной окружности 13.

Задача 10. Используя шифр Сцитала расшифровать сообщение: МААМОМООТТЖОРУСЖНТМГПНМЕТЫЗКИЕОНОЫОУКОЙ.

Материалы для проведения промежуточной аттестации:

Седьмой семестр.
1. Вид промежуточной аттестации – экзамен.
2. Форма проведения - устный опрос.
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень тем и вопросов, выносимых на промежуточную аттестацию:

1) Шифр Виженера.
2) Шифратор «Энигма»
3) Шифратор «Хагелин»
4) Математическая теория криптографии Клода Шеннона.
5) Телефонные шифраторы.
6) Стандарт шифрования данных (DES).
7) Конфиденциальность.
8) Целостность.
9) Аутентификация.
10) Имитостойкость.
11) Ключи, ключевая система, распределение ключей.
12) Предварительное и линейное шифрование.
13) Физические и организационные меры при использовании шифрсистем.
14) Криптографическая стойкость шифров.
15) Имитостойкость и помехоустойчивость шифров.
16) Шифры, не распространяющие искажений.
17) Шифры перестановки и их свойства.
18) Элементы криптоанализа шифров перестановки.
19) Шифры замены и их свойства.
20) Криптоанализ шифра простой замены.
21) Многоалфавитные шифры замены.
22) Шифры гаммирования.
23) Повторное использование гаммы.
24) Криптоанализ шифра Виженера.
25) Ошибки шифровальщика.
26) Системы шифрования с открытыми ключами.
27) Шифрсистема RSA.
28) Электронная цифровая подпись.

29) Цифровые подписи на основе шифрсистем с открытыми ключами
30) Цифровая подпись Фиата-Шамира.
31) Цифровая подпись Эль-Гамаля.
32) Одноразовые цифровые подписи.
33) Шифрование в телефонии.
34) Скремблирование.
35) Частотные преобразования речевого сигнала.
36) Алгебраическая модель шифра замены.
37) Алгебраическая модель шифра перестановки.
38) Алгебраическая модель шифра RSA.
39) Вероятностная модель шифрования.
40) Алгебраические модели открытого текста.
41) Вероятностные модели открытого текста.
42) Критерии распознавания открытого текста.
43) Энтропия и избыточность языка.
44) Расстояние единственности.
45) Принципы построения криптографических алгоритмов блочных шифров.
46) Криптографические параметры «перемешивающих» и «рассеивающих» блоков.
47) Композиции шифров.
48) Синтез шифров DES алгоритма.
49) Принципы построения криптографических алгоритмов поточного шифрования.
50) Аппаратные реализации шифров.
51) Программные реализации шифров.
52) Методы получения случайных и псевдослучайных последовательностей.
53) Линейные регистры сдвига.
54) Композиции линейных регистров сдвига.
55) Вопросы организации сетей засекреченной связи. Ключевые системы.
56) Криптографические хеш-функции.
57) Функции хэширования и целостность данных.
58) Криптографические протоколы.
59) Протоколы распределения ключей.
60) Протоколы идентификации.

Перечень практических заданий, выносимых на промежуточную аттестацию:

Открытый ключ системы RSA задается числами n=33 , e=7. Используя этот ключ было получено шифрованное сообщение {9; 1; 29}.

Найти исходное открытое сообщение $\{M_1; M_2; M_3\}$.

Для сообщения M=474 , используя систему RSA (n=527 , e=7), вычислить цифровую подпись S.

Используя алгоритм Диффи-Хеллмана по заданным значениям: модуль - m=61 , основание a=5, секретные ключи абонентов - x=7, y=11, вычислить значение открытых ключей абонентов -K_x и K_y.

Используя алгоритм Диффи-Хеллмана по заданным значениям: модуль - m=61 , основание a=5, секретные ключи абонентов - x=7, y=11, вычислить значение общего ключа.

Открытый ключ системы RSA задается числами n=33 , e=7. Необходимо найти секретный ключ d.

Для сообщения M=297 , используя систему RSA (n=527 , e=343), вычислить цифровую подпись S.

Открытый ключ системы RSA задается числами n=33 , e=3. Используя этот ключ было получено шифрованное сообщение {3; 1; 2}.

Найти исходное открытое сообщение $\{M_1; M_2; M_3\}$.

Используя алгоритм Диффи-Хеллмана по заданным значениям: модуль - m=11 , основание a=7, секретные ключи абонентов - x=3, y=6, вычислить значение общего ключа.

Используя алгоритм Диффи-Хеллмана по заданным значениям: модуль - m=59 , основание a=3, секретные ключи абонентов - x=7, y=11, вычислить значение открытых ключей абонентов -K_x и K_y

Открытый ключ системы RSA задается числами n=91 , e=29. Найти соответствующий секретный ключ.

Ключ зашифрования системы RSA (n=527 , e=7), вычислить ключ расшифрования.

Секретный ключ системы RSA задается числами n=91 , d=5. Найти соответствующий открытый ключ.

Используя шифр Виженера зашифровать фразу: FINIS CORONAT OPUS с помощью ключевого слова VERBA.

Используя шифр Виженера расшифровать сообщение: AMEJSXSIPNVXFQUN с помощью ключевого слова VERBA.

Используя шифр гаммирования зашифровать фразу: ALTER EGO с помощью случайной равновероятной гаммы UDLGOXTA

Используя шифр гаммирования расшифровать сообщение: UOEKFBZO с помощью случайной равновероятной гаммы UDLGOXTA

Используя шифр Цезаря зашифровать фразу: THE POETRY IS NEVER DEAD с помощью ключа D

Используя шифр Цезаря расшифровать сообщение: WKH SRHWUB LV QHYHU GHDG. Ключ неизвестен.

Используя шифр Сцитала зашифровать фразу: МУЗА СКАЖИ МНЕ О ТОМ МНОГООПЫТНОМ МУЖЕ КОТОРЫЙ при помощи цилиндра с длинной окружности 13.

Используя шифр Сцитала расшифровать сообщение: МААМОМООТТЖОРУСЖНТМГПНМЕТЫЗКИЕОНОЫОУКОЙ.