Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Радиофизический факультет

УТВЕРЖДЕНО:
Декан
А. Г. Коротаев

Оценочные материалы по дисциплине

Защита информации

по направлению подготовки / специальности

03.03.03 Радиофизика

Направленность (профиль) подготовки/ специализация:
Киберфизические системы, прикладная электроника и квантовые технологии

Форма обучения
Очная

Квалификация
Радиофизик-кибернетик, преподаватель. Разработчик киберфизических и квантовых систем

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
О.А. Доценко

Председатель УМК
А.П. Коханенко

Томск – 202

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

БК-1 Способен применять общие и специализированные компьютерные программы при решении задач профессиональной деятельности.

ОПК-3 Способен использовать информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

РОБК 1.1 Знает правила и принципы применения общих и специализированных компьютерных программ для решения задач профессиональной деятельности

РОБК 1.2 Умеет применять современные IT-технологии для сбора, анализа и представления информации; использовать в профессиональной деятельности общие и специализированные компьютерные программы

РООПК 3.1 Знает современные информационные технологии и программные средства при решении задач профессиональной деятельности.

РООПК 3.2 Умеет соблюдать требования информационной безопасности при использовании современных информационных технологий и программного обеспечения

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– тест;
– отчеты по практическим занятиям.

Тест (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

1. Какие исторические шифры Вы знаете:
   а) шифры замены;
   б) шифры перестановки;
   в) шифра гаммирования;
   г) шифры подмены;
   д) шифры подстановки.
2. Под конфиденциальностью информации понимается:
   а) доступность только ограниченному кругу пользователей;
   б) сохранение своего содержания/структуры в процессе хранения/передачи;
   в) совершение действия незаметно для других;
   г) принадлежность источнику информации;
   д) доступность в соответствии с временными потребностями пользователя.
3. Под целостностью информации понимается:
   а) доступность только ограниченному кругу пользователей;
   б) сохранение своего содержания/структуры в процессе хранения/передачи;
   в) совершение действия незаметно для других;
   г) принадлежность источнику информации;
   д) доступность в соответствии с временными потребностями пользователя.
4. Под неотслеживаемостью информации понимается:
   а) доступность только ограниченному кругу пользователей;
   б) сохранение своего содержания/структуры в процессе хранения/передачи;
   в) совершение действия незаметно для других;
   г) принадлежность источнику информации;
   д) доступность в соответствии с временными потребностями пользователя.
5. Под достоверностью информации понимается:
   а) доступность только ограниченному кругу пользователей;

б) сохранение своего содержания/структуры в процессе хранения/передачи;
в) совершение действия незаметно для других;
г) принадлежность источнику информации;
д) доступность в соответствии с временными потребностями пользователя.

6. Под оперативностью информации понимается:
а) доступность только ограниченному кругу пользователей;
б) сохранение своего содержания/структуры в процессе хранения/передачи;
в) совершение действия незаметно для других;
г) принадлежность источнику информации;
д) доступность в соответствии с временными потребностями пользователя.

7. Методы защиты информации называются стеганографическими, если
а) сам факт передачи информации замаскировывается;
б) защищают от разрушения встраиваемых и внешних средств защиты;
в) защищают от неправомочных действий пользователей;
г) защищают от несанкционированного доступа к информации.

8. Методы защиты информации называются физическими, если
а) сам факт передачи информации замаскировывается;
б) защищают от разрушения встраиваемых и внешних средств защиты;
в) защищают от неправомочных действий пользователей;
г) защищают от несанкционированного доступа к информации.

9. Методы защиты информации называются организационными, если
а) сам факт передачи информации замаскировывается;
б) защищают от разрушения встраиваемых и внешних средств защиты;
в) защищают от неправомочных действий пользователей;
г) защищают от несанкционированного доступа к информации.

10. Методы защиты информации называются криптографическими, если
а) сам факт передачи информации замаскировывается;
б) защищают от разрушения встраиваемых и внешних средств защиты;
в) защищают от неправомочных действий пользователей;
г) защищают от несанкционированного доступа к информации.

11. Существует ли абсолютно стойкий шифр:
а) да, если он удовлетворяет трем условиям, сформулированным Шенноном;
б) всякий шифр является абсолютно стойким;
в) абсолютно стойкого шифра не существует.

12. Выберите правильные характеристики DES:
а) длина ключа 32 бита;
б) длина ключа 56 битов;
в) длина блока открытого текста 64 бита;
г) длина блока открытого текста 32 бита;
д) количество раундов 16;
е) количество раундов 32.

13. Выберите правильные характеристики ГОСТ 28147-:
а) длина ключа 32 бита;
б) длина ключа 256 битов;
в) длина блока открытого текста 64 бита;
г) длина блока открытого текста 32 бита;
д) количество раундов 16;
е) количество раундов 32.

14. Аутентификация необходима для того, чтобы:
а) идентифицировать участника протокола;
б) доказать авторство электронного документа;
зашифровать электронный документ

в) в электронном информационном пространстве она вообще не нужна.

15. Электронно-цифровая подпись предназначена для того, чтобы:

а) доказать подлинность электронного документа;

б) зашифровать электронный документ;

в) расшифровать электронный документ;

г) в электронном информационном пространстве она вообще не нужна.

16. Метки времени в электронных документах используются, чтобы:

а) предотвратить повторное использование электронного документа;

б) использовать электронный документ в определенную дату и время;

в) вообще не использовать электронный документ.

17. Шифротекст «lx anmmhd hr nudq sgd nbdzm» получен шифром Цезаря при к=-1. Определите исходный открытый текст.

а) my bonnie is over the ocean;

б) naecoehtrevosieinnobym;

в) lx anmmhd hr nudq sgd nbdzm.

18. Что получится в результате шифрования открытого текста «authentication» шифром Виженера с ключом «is»?

а) imbzmfbaksbawf;

б) imthentication;

в) authentication.

19. Что получится в результате шифрования открытого текста «protocol» шифром гаммирования с автоключом, если в качестве ключа выступает «a»?

а) pgfhhqqz;

б) pgfhqz;

в) protocol.

Ключи: 1 а, б, в), 2 а), 3 б), 4 в), 5 г), 6 д), 7 а), 8 б), 9 в), 10 г), 11 а), 12 б, в, д), 13 б, в, е), 14 а), 15 а), 16 а), 17 а), 18 а), 19 а).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на 10 вопросов.

Отчеты по практическим занятиям (РОБК 1.2, РООПК 3.2)

Тема «Шифр Цезаря»

Пример задания:

Сделайте программную реализацию алгоритма шифрования/расшифрования. Проверьте правильность программной реализации.

Зашифруйте открытый текст «authentication», используя ключ k=3. Сообщите шифротекст и ключ товарищу (для расшифрования).

Возьмите шифротекст, полученный товарищем, и используемый им ключ, расшифруйте сообщение. Сравните полученное сообщение с исходным открытым текстом.

Результат выполнения работы определяется оценками «зачтено» и «незачтено».

Оценка «зачтено» выставляется, если задание выполнено в соответствии с указанными требованиями (все недочеты устранены), при расшифровании получается исходный открытый текст.

Оценка «незачтено» выставляется, если задание не выполнено.

Тема «Шифр Виженера»

Пример задания:

Сделайте программную реализацию алгоритма шифрования/расшифрования. Проверьте правильность программной реализации.

Зашифруйте открытый текст «authentication», используя ключ *k*=the. Сообщите шифротекст и ключ товарищу (для расшифрования).

Возьмите шифротекст, полученный товарищем, и используемый им ключ, расшифруйте сообщение. Сравните полученное сообщение с исходным открытым текстом.

Результат выполнения работы определяется оценками «зачтено» и «незачтено».

Оценка «зачтено» выставляется, если задание выполнено в соответствии с указанными требованиями (все недочеты устранены), при расшифровании получается исходный открытый текст.

Оценка «незачтено» выставляется, если задание не выполнено.

Тема «Шифр гаммирования с автоключом»

Пример задания:

Сделайте программную реализацию алгоритма шифрования/расшифрования. Проверьте правильность программной реализации.

Зашифруйте открытый текст «mybonnieisovertheocean», используя ключ *k*=h. Сообщите шифротекст и ключ товарищу (для расшифрования).

Возьмите шифротекст, полученный товарищем, и используемый им ключ, расшифруйте сообщение. Сравните полученное сообщение с исходным открытым текстом.

Результат выполнения работы определяется оценками «зачтено» и «незачтено».

Оценка «зачтено» выставляется, если задание выполнено в соответствии с указанными требованиями (все недочеты устранены), при расшифровании получается исходный открытый текст.

Оценка «незачтено» выставляется, если задание не выполнено.

Тема «Книжный шифр гаммирования»

Пример задания:

Сделайте программную реализацию алгоритма шифрования/расшифрования. Проверьте правильность программной реализации.

Зашифруйте открытый текст «mybonnieisoverthesea», используя ключ *k*= kinematicsanddynamics. Сообщите шифротекст и ключ товарищу (для расшифрования).

Возьмите шифротекст, полученный товарищем, и используемый им ключ, расшифруйте сообщение. Сравните полученное сообщение с исходным открытым текстом.

Результат выполнения работы определяется оценками «зачтено» и «незачтено».

Оценка «зачтено» выставляется, если задание выполнено в соответствии с указанными требованиями (все недочеты устранены), при расшифровании получается исходный открытый текст.

Оценка «незачтено» выставляется, если задание не выполнено.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзаменационный билет состоит из двух частей.

Первый вопрос проверяет РОБК 1.1, 1.2. Второй вопрос проверяет РООПК 3.1, 3.2. Ответы на вопросы даются в развернутой форме.

Перечень теоретических вопросов:

1. Основные понятия и задачи криптографии.
2. Основные криптоаналитические атаки.
3. Стойкость криптоалгоритмов.
4. Криптографическая система DES.
5. Криптографическая система ГОСТ 28147-89.

6. Режимы использования блочных шифров.
7. Криптографическая система RSA.
8. Шифры простой замены.
9. Криптоанализ шифров простой замены.
10. Шифры многоалфавитной замены.
11. Шифры перестановки.
12. Криптоанализ шифров перестановки.
13. Организация секретной связи с использованием симметричной и несимметричной криптосистем**.**
14. Математическая модель шифра по К. Шеннону.
15. Поточные шифры.
16. Блочные шифры: принципы построения блочных шифров.
17. Криптографические протоколы.
18. Протоколы аутентификации.
19. Электронно-цифровая подпись.

Критерии оценивания:

Результаты зачета определяются оценками «зачтено», «незачтено».

Оценка «зачтено» выставляется, если даны правильные ответы на оба вопроса билета.

Оценка «незачтено» выставляется, если хотя бы на один из вопросов билета не дано ответа.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест

1. Какие исторические шифры Вы знаете (3 типа шифров): (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) шифры замены;
б) шифры перестановки;
в) шифра гаммирования;
г) шифры подмены;
д) шифры подстановки.

2. Под конфиденциальностью понимается свойство информации: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) быть доступной только ограниченному кругу пользователей;
б) сохранять свое содержание/структуру в процессе хранения/передачи;
в) совершать действия незаметно для других.

3. Методы защиты информации называются стеганографическими, если: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) сам факт передачи информации замаскировывается;
б) защищают от разрушения встраиваемых и внешних средств защиты;
в) защищают от неправомочных действий пользователей.

4. Существует ли абсолютно стойкий шифр: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) да, если он удовлетворяет трем условиям, сформулированным Шенноном;
б) любой шифр является абсолютно стойким;
в) абсолютно стойкого шифра не существует.

5. В алгоритме шифрования DES длина блока открытого текста равна: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) 32 бита;
б) 64 бита;
в) 128 битов;

г) может быть задана произвольно.

6. В алгоритме шифрования DES длина ключа равна: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) 32 бита;

б) 56 битов;

в) 128 битов;

г) может быть задана произвольно.

7. В алгоритме шифрования ГОСТ 28147-89 длина блока открытого текста равна: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) 32 бита;

б) 64 бита;

в) 128 битов;

г) может быть задана произвольно.

8. В алгоритме шифрования ГОСТ 28147-89 длина ключа равна: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) 32 бита;

б) 128 битов;

в) 256 битов;

г) может быть задана произвольно.

9. Электронно-цифровая подпись предназначена для того, чтобы: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) доказать подлинность электронного документа;

б) расшифровать электронный документ;

в) в электронном информационном пространстве она вообще не нужна.

10. Аутентификация необходима для того, чтобы: (РОБК 1.1, 1.2, РООПК 3.1, 3.2)

а) идентифицировать участника протокола;

б) доказать авторство электронного документа;

в) в электронном информационном пространстве она вообще не нужна.

Ключи: 1 а, б, в), 2 а), 3 а), 4 а), 5 б), 6 б), 7 б), 8 в), 9 а), 10 а).

Информация о разработчиках

Прокопенко Светлана Анатольевна, канд. техн. наук, доцент, ТГУ, доцент