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

03.03.03 Радиофизика

Направленность (профиль) подготовки:
Радиофизика, электроника и информационные системы

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
М.Л. Громов

Председатель УМК
А.П. Коханенко

Томск – 2025

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

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности..

ПК-2 Способен проводить математическое моделированию процессов в приборах и устройствах радиофизики и электроники, владеть современными отечественными и зарубежными пакетами программ при решении при решении профессиональных задач..

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 3.1 Использует современные информационные технологии и программные средства при решении задач профессиональной деятельности.

ИОПК 3.2 Соблюдает требования информационной безопасности при использовании современных информационных технологий и программного обеспечения.

ИПК 2.1 Понимает принцип действия и модели разрабатываемого радиоэлектронного прибора или устройства.

ИПК 2.2 Применяет в профессиональной деятельности различные численные методы, в том числе реализованные в готовых библиотеках при решении конкретных радиофизических задач.

ИПК 2.3 Владеет современными пакетами программ при решении задач в области радиофизики и радиоэлектроники.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– тест;
– отчеты по лабораторным работам.

Тест (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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 лабораторным работам (ИОПК 3.1, ИПК 2.2, 2.3)

Лабораторная работа «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 лабораторной 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.

Лабораторная работа «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 лабораторной 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.

Лабораторная работа «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 лабораторной 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.

Лабораторная работа «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 лабораторной 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 ИОПК 3.1, ИОПК 3.2. Второй вопрос проверяет ИПК 2.1, ИПК 2.2, ИПК 2.3. 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): (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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

2. Под конфиденциальностью понимается свойство информации: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

а) 32 бита;

б) 64 бита;

в) 128 битов;

г) может быть задана произвольно.

6. В алгоритме шифрования DES длина ключа равна: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.32)

а) 32 бита;

б) 64 бита;

в) 128 битов;

г) может быть задана произвольно.

8. В алгоритме шифрования ГОСТ 28147-89 длина ключа равна: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

а) 32 бита;

б) 128 битов;

в) 256 битов;

г) может быть задана произвольно.

9. Электронно-цифровая подпись предназначена для того, чтобы: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

а) доказать подлинность электронного документа;

б) расшифровать электронный документ;

в) в электронном информационном пространстве она вообще не нужна.

10. Аутентификация необходима для того, чтобы: (ИОПК 3.1, 3.2, ИПК 2.1 – 2.3)

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