

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ** «**ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

**(ОЦЕНОЧНЫЕ СРЕДСТВА)**

**для проведения текущего контроля и промежуточной аттестации**

по дисциплине

«Информационная безопасность и защита информации»

для обучающихся по направлению подготовки (специальности)

09.03.03 «Прикладная информатика»

профиль Прикладная информатика в информационной сфере

20\_\_ года набора

Ростов-на-Дону

20\_\_

**Лист согласования**

Оценочные материалы (оценочные средства) по дисциплине Информационная безопасность и защита информации составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

Рассмотрены и одобрены на заседании кафедры «Информационные технологии» протокол № \_\_\_

от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г

Разработчики оценочных материалов (оценочных средств)

Доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Н. Левченков

подпись

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Б.В. Соболь

подпись

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**Согласовано:**

Зам. генерального директора ООО "Сайбериум"

\_\_\_\_\_\_\_\_\_\_\_\_С.Е.Перфишин

подпись

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Генеральный директор ООО "IT-Компания Союз"

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.М.Сотниченко

подпись

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**1 Паспорт оценочных материалов (оценочных средств)**

Оценочные материалы (оценочные средства) прилагаются к рабочей программе дисциплины и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения обучающимся установленных результатов обучения.

Оценочные материалы (оценочные средства) используются при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся.

* 1. **Перечень компетенций, формируемых дисциплиной,**

**с указанием этапов их формирования в процессе освоения ОПОП**

Перечень компетенций, формируемых в процессе изучения дисциплины:

ОПК-3.1: Выполняет стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

ОПК-3.2: Применяет основные требования информационной безопасности в рамках реализации информационной и библиографической культуры для решения поставленных задач в профессиональной деятельности

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения (табл. 1).

Таблица 1 ‒ Формирование компетенций в процессе изучения дисциплины

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Код компетенции | Уровень освоения | Дескрипторы компетенции  (результаты обучения, показатели достижения результата обучения, которые обучающийся может продемонстрировать) | Вид учебных занятий, работы,  формы и методы обучения, способствующие формированию и развитию компетенции | Контролируемые разделы и темы дисциплины | Оценочные материалы (оценочные средства), используемые для оценки уровня сформированности компетенции | Критерии оценивания компетенций |
| ОПК-3.1 | **Знать** |  | Лек., лаб. раб., сам. раб.  Интерактивная лекция | Разделы 1-4 | Контрольные вопросы | Ответы на контрольные вопросы; Выполнение лабораторных работ и их защита по контрольным вопросам в форме собеседования. |
| Уровень 1: | Методы работы с информацией |
| Уровень 2: | Общие требования к составлению библиографического описания документов с позиции требований информационного поиска |
| Уровень 3: | Методы решения стандартных задач профессиональной деятельности |
| **Уметь** |  | Лек., лаб. раб., сам. раб.  Работа в группах | Лабораторные работы |
| Уровень 1: | Использовать средства информационно-коммуникационных технологий для поиска и анализа информации |
| Уровень 2: | Методы решения стандартных задач профессиональной деятельности |
| Уровень 3: | Осуществлять обмен информации с удаленными компьютерами, доступ к ресурсам Internet, поиск информации и анализ данных |
| **Владеть** |  | Лек., лаб. раб., сам. раб.  Работа в группах | Лабораторные работы |
| Уровень 1: | Навыками решения стандартных задач профессиональной деятельности |
| Уровень 2: | Подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе |
| Уровень 3: | Методами формирования и использования баз данных и информационно-справочных систем при анализе различных данных, ресурсов телекоммуникационных технологий и глобальной сети Internet |
| ОПК-3.2 | **Знать** |  | Лек., лаб. раб., сам. раб.  Интерактивная лекция | Разделы 1-4 | Контрольные вопросы | Ответы на контрольные вопросы; Выполнение лабораторных работ и их защита по контрольным вопросам в форме собеседования. |
| Уровень 1: | Основные требования к обеспечению информационной безопасности для решения задач в профессиональной деятельности |
| Уровень 2: | Основные методы обеспечения информационной безопасности для решения задач в профессиональной деятельности |
| Уровень 3: | Законодательный уровень информационной безопасности, математические основы криптографии (теорию информации, понятие энтропии и неопределенности, теорию сложности, теорию чисел) |
| **Уметь** |  | Лек., лаб. раб., сам. раб.  Работа в группах | Лабораторные работы |
| Уровень 1: | Использовать требования к обеспечения информационной безопасности для решения задач в профессиональной деятельности |
| Уровень 2: | Использовать методы обеспечения информационной безопасности для решения задач в профессиональной деятельности |
| Уровень 3: | Разрабатывать политику информационной безопасности, проводить оценку угроз безопасности объекта информатизации, проектировать системы защиты информации |
| **Владеть** |  | Лек., лаб. раб., сам. раб.  Работа в группах | Лабораторные работы |
| Уровень 1: | Навыками безопасной работы с информационными технологиями в рамках библиографической культуры для решения задач профессиональной деятельности |
| Уровень 2: | Средствами защиты информации в информационно-телекоммуникационных сетях. |
| Уровень 3: | Навыками программирования алгоритмов криптографической защиты информации. |

* 1. **Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

Оценивание результатов обучения по дисциплине осуществляется в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся.

По дисциплине «*Информационная безопасность и защита информации»* предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины); промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающихся. Текущий контроль служит для оценки объёма и уровня усвоения обучающимся учебного материала одного или нескольких разделов дисциплины (модуля) в соответствии с её рабочей программой и определяется результатами текущего контроля знаний обучающихся.

Текущий контроль осуществляется два раза в семестр по календарному графику учебного процесса.

Текущий контроль предполагает начисление баллов за выполнение различных видов работ.Результаты текущего контроля подводятся по шкале балльно-рейтинговой системы. Регламент балльно-рейтинговой системы определен Положением о системе «Контроль успеваемости и рейтинг обучающихся».

Текущий контроль является результатом оценки знаний, умений, навыков и приобретенных компетенций обучающихся по всему объёму учебной дисциплины, изученному в семестре, в котором стоит форма контроля в соответствии с учебным планом.

Текущий контроль успеваемости предусматривает оценивание хода освоения дисциплины: теоретических основ и практической части.

Промежуточная аттестация по дисциплине «*Информационная безопасность и защита информации*» проводится в форме экзамена. Защита лабораторных и практических работ является обязательной частью промежуточной аттестации, без выполнения которой обучающиеся не допускаются к промежуточной аттестации.

В табл. 2 приведено весовое распределение баллов и шкала оценивания по видам контрольных мероприятий.

Таблица 2 ‒ Весовое распределение баллов и шкала оценивания по видам контрольных мероприятий

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Текущий контроль  (50 баллов) | | | | | | Промежуточная аттестация  (50 баллов) | Итоговое количество баллов по результатам текущего контроля и промежуточной аттестации |
| Блок 1 | | | Блок 2 | | |
| Лекционные занятия (X1) | Практические занятия (Y1) | Лабораторные занятия (Z1) | Лекционные занятия (X2) | Практические занятия (Y2) | Лабораторные занятия (Z2) | от 0 до 50 баллов | Менее 41 балла –  неудовлетворительно  41-60 баллов – удовлетворительно  61-80 баллов – хорошо;  81-100 баллов ‒ отлично |
|  |  | 25 |  |  | 25 |
| Сумма баллов за 1 блок = 20 | | | Сумма баллов за 2 блок = 30 | | |

Для определения фактических оценок каждого показателя выставляются следующие баллы (табл.3):

Таблица 3– Распределение баллов по дисциплине

|  |  |  |
| --- | --- | --- |
| Вид учебных работ по дисциплине | ***Количество баллов*** | |
| ***1 блок*** | ***2 блок*** |
| *Текущий контроль (50 баллов)* | | |
| Выполнение лабораторных работ, включая подготовку отчета и защиту. | *25* | *25* |
| *Промежуточная аттестация (50 баллов)* | | |
| Экзамен по дисциплине «*Информационная безопасность и защита информации*» проводится в письменной форме в виде ответов на вопросы для промежуточной аттестации. Задание для экзамена состоит из 3 вопросов. Первый позволяет оценить теоретические знания, а второй и третий – умения и навыки. Правильный ответ на первый вопрос оценивается в 15 баллов, второй – в 15 баллов, третий – в 20 баллов. За неверно выполненное задание – 0 баллов. | | |
| **Сумма баллов по дисциплине 100 баллов** | | |

Экзамен является формой итоговой оценки качества освоения обучающимся образовательной программы по дисциплине в целом или по разделу дисциплины. По результатам экзамена обучающемуся выставляется оценка «отлично», «хорошо», «удовлетворительно», или «неудовлетворительно».

Оценка «отлично» (81-100 баллов) выставляется обучающемуся, если:

- обучающийся набрал по текущему контролю необходимые и достаточные баллы для выставления оценки автоматом;

- обучающийся знает, понимает основные положения дисциплины, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения;

- обучающийся анализирует элементы, устанавливает связи между ними, сводит их в единую систему, способен выдвинуть идею, спроектировать и презентовать свой проект (решение);

- ответ обучающегося по теоретическому и практическому материалу, содержащемуся в вопросах экзаменационного билета, является полным, и удовлетворяет требованиям программы дисциплины;

- обучающийся продемонстрировал свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей дисциплины;

- на дополнительные вопросы преподавателя обучающийся дал правильные ответы.

Компетенция (и) или ее часть (и) сформированы на высоком уровне (уровень 3) (см. табл. 1).

Оценка «хорошо» (61-80 баллов) выставляется обучающемуся, если:

- обучающийся знает, понимает основные положения дисциплины, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения; анализирует элементы, устанавливает связи между ними;

- ответ по теоретическому материалу, содержащемуся в вопросах экзаменационного билета, является полным, или частично полным и удовлетворяет требованиям программы, но не всегда дается точное, уверенное и аргументированное изложение материала;

- на дополнительные вопросы преподавателя обучающийся дал правильные ответы;

- обучающийся продемонстрировал владение терминологией соответствующей дисциплины.

Компетенция (и) или ее часть (и) сформированы на среднем уровне (уровень 2) (см. табл. 1).

Оценка «удовлетворительно» (41-60 баллов) выставляется обучающемуся, если:

- обучающийся знает и воспроизводит основные положения дисциплины в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;

- обучающийся продемонстрировал базовые знания важнейших разделов дисциплины и содержания лекционного курса;

- у обучающегося имеются затруднения в использовании научно-понятийного аппарата в терминологии курса;

- несмотря на недостаточность знаний, обучающийся имеется стремление логически четко построить ответ, что свидетельствует о возможности последующего обучения.

Компетенция (и) или ее часть (и) сформированы на базовом уровне (уровень 1) (см. табл. 1).

Оценка «неудовлетворительно» (менее 41 балла) выставляется обучающемуся, если:

- обучающийся имеет представление о содержании дисциплины, но не знает основные положения (темы, раздела, закона и т.д.), к которому относится задание, не способен выполнить задание с очевидным решением, не владеет навыками проведения анализа возможностей реализации требований к программному обеспечению; оценки времени и трудоемкости реализации требований к программному обеспечению; согласования требований к программному обеспечению с заинтересованными сторонами; оценки и согласования сроков выполнения поставленных задач; разработки и согласования технических спецификаций на программные компоненты и их взаимодействие с архитектором программного обеспечения; распределения заданий между программистами в соответствии с техническими спецификациями; осуществления контроля выполнения заданий; формирования и предоставления отчетности в соответствии с установленными регламентами; разработки, изменения и согласования архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения; проектирования структур данных; проектирования баз данных; проектирования программных интерфейсов;

- у обучающегося имеются существенные пробелы в знании основного материала по дисциплине;

- в процессе ответа по теоретическому материалу, содержащемуся в вопросах экзаменационного билета, допущены принципиальные ошибки при изложении материала.

Компетенция(и) или ее часть (и) не сформированы.

**2. Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**2.1 Задания для оценивания результатов обучения в виде знаний**

Контрольные вопросы к текущей аттестации:

1 рейтинг:

1. Термин «Информационная безопасность».

2. Важность и сложность проблемы информационной безопасности.

3. Грани информационной безопасности.

4. Наиболее распространенные угрозы информационной безопасности.

5. Основные угрозы доступности.

6. Классификации вредоносного ПО.

7. Окно опасности.

8. Наиболее распространенные угрозы информационно безопасности.

9. Основные угрозы целостности.

10. Наиболее распространенные угрозы информационно безопасности.

11. Основные угрозы конфиденциальности.

12. Уровни информационной безопасности. Законодательный уровень.

13. Задачи решаемы на законодательном уровне ИБ.

14. Российское законодательство в области информационной безопасности.

15. Конституция. Гражданский кодекс. Уголовный кодекс.

16. Требования к алгоритмам асимметричного шифрования.

17. Российское законодательство в области информационной безопасности.

18. Закон о «Государственной тайне».

19. Закон «Об информации, информационных отношениях и о защите информации.»

20. Оранжевая книга.

21. Классы оранжевой книги.

22. Защита персональных данных.

23. Гармонизированные критерии Европейских стран.

24. Теория чисел.

25. Простые и взаимнопростые числа.

26. Наибольший общий делитель. Алгоритмы.

27. Арифметика в классах вычетов.

28. Операции сложения и умножения.

29. Аддитивный обратный и мультипликативный обратный.

30. Теорема Ферма и Эйлера в приложении к классам вычетов.

31. Генерация простых чисел. Принципы. Алгоритмы.

32. Квадратичные вычеты и квадратичные невычеты. Главный корень.

33. Симметричное шифрование.

34. Сеть Фейстеля.

2 рейтинг:

1. Режимы выполнения алгоритмов симметричного шифрования.

2. Алгоритмы AES.

3. Претенденты. Характеристики. Выбор.

4. Асимметричное шифрование.

5. Ключи асимметричного шифрования.

6. Достоинства и недостатки асимметричного шифрования.

7. Цифровая подпись.

8. Прозрачная и непрозрачная цифровая подпись.

9. Принципы формирования и алгоритмы цифровой подписи.

10. Распределение ключей в современной информационной системе.

11. Требования к алгоритмам асимметричного шифрования.

12. Хэш функции.

13. Требования к хеш функциям.

14. Теория информации.

15. Энтропия и неопределенность.

16. Избыточность.

17. Хэш функции.

18. Простые хэш функции.

19. Парадокс дней рождений.

20. Коды аутентификации MAC. Применение.

21. Китайская теорема об остатках. Её роль в криптографии. Принципы операций при применении теоремы.

22. Индексы.

23. Дискретные логарифмы в классах вычетов.

24. Совместное применение алгоритмов симметричного и асимметричного шифрования.

25. Алгоритмы асимметричного шифрования.

26. Цифровая подпись.

27. Принципы формирования цифровой подписи.

28. Протоколы.

29. Основные определения протоколов.

30. Безопасность протоколов.

31. Протоколы с посредником.

32. Протоколы с арбитром.

33. Самодостаточные протоколы.

34. Атаки на протокол.

35. Пример атаки на протокол.

36. Протокол KERBEROS.

Контрольные вопросы к промежуточной аттестации:

1. Термин «Информационная безопасность». Важность и сложность проблемы информационной безопасности. Грани информационной безопасности.

2. Наиболее распространенные угрозы информационной безопасности. Основные угрозы доступности.

3. Классификации вредоносного ПО. Окно опасности.

4. Наиболее распространенные угрозы информационно безопасности. Основные угрозы целостности.

5. Наиболее распространенные угрозы информационно безопасности. Основные угрозы конфиденциальности.

6. Уровни информационной безопасности. Законодательный уровень. Задачи решаемы на законодательном уровне ИБ.

7. Российское законодательство в области информационной безопасности. Конституция. Гражданский кодекс. Уголовный кодекс.

8. Требования к алгоритмам асимметричного шифрования.

9. Российское законодательство в области информационной безопасности. Закон о «Государственной тайне». Закон «Об информации, информационных отношениях и о защите информации.»

10. Оранжевая книга. Классы оранжевой книги.

11. Защита персональных данных.

12. Гармонизированные критерии Европейских стран.

13. Теория чисел. Простые и взаимнопростые числа. Наибольший общий делитель. Алгоритмы.

14. Арифметика в классах вычетов. Операции сложения и умножения. Аддитивный обратный и мультипликативный обратный.

15. Теорема Ферма и Эйлера в приложении к классам вычетов.

16. Генерация простых чисел. Принципы. Алгоритмы.

17. Квадратичные вычеты и квадратичные невычеты. Главный корень.

18. Симметричное шифрование. Сеть Фейстеля.

19. Режимы выполнения алгоритмов симметричного шифрования.

20. Алгоритмы AES. Претенденты. Характеристики. Выбор.

21. Асимметричное шифрование. Ключи асимметричного шифрования. Достоинства и недостатки асимметричного шифрования.

22. Цифровая подпись. Прозрачная и непрозрачная. Принципы формирования и алгоритмы.

23. Распределение ключей в современной информационной системе.

24. Требования к алгоритмам асимметричного шифрования.

25. Хэш функции. Требования к хеш функциям.

26. Теория информации. Энтропия и неопределенность. Избыточность

27. Хэш функции. Простые хэш функции. Парадокс дней рождений.

28. Коды аутентификации MAC. Применение.

29. Китайская теорема об остатках. Её роль в криптографии. Принципы операций при применении теоремы.

30. Индексы. Дискретные логарифмы в классах вычетов.

31. Совместное применение алгоритмов симметричного и асимметричного шифрования.

32. Алгоритмы асимметричного шифрования.

33. Цифровая подпись. Принципы формирования.

34. Протоколы. Основные определения протоколов. Безопасность протоколов.

35. Протоколы с посредником.

36. Протоколы с арбитром.

37. Самодостаточные протоколы.

38. Атаки на протокол. Пример атаки на протокол.

39. Протокол KERBEROS.

Критерии оценивания ответа, обучающегося на контроле:

|  |  |
| --- | --- |
| Балл | Критерии |
| 50 | полно излагает изученный материал, дает правильное определение языковых понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебного материала, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка. |
| 40 | ответ полный и правильный на основании изученной теории; материал изложен в определенной логической последовательности, но допущены 2-3 несущественные ошибки, исправленные по требованию преподавателя; |
| 30 | ответ полный, но при этом допущена существенная ошибка, или ответ неполный, неясный; |
| 20 | при ответе обнаружено непонимание обучающийсяом основного содержания учебного материала или допущены существенные ошибки, которые обучающийся не может исправить при наводящих вопросах преподавателя; не проявлены умения использовать нормативную, справочную, дополнительную литературу. |
| 1 | ответ на 95% неправильный или не соответствует поставленному вопросу. |

**2.2 Задания для оценивания результатов в виде владений и умений**

Темы лабораторных работ:

1. Законодательство РФ в области информационной безопасности
2. Реализация дискреционной модели политики безопасности
3. Количественная оценка стойкости парольной защиты
4. Методы и программная реализация алгоритмов шифрования
5. Ассиметричные алгоритмы шифрования данных
6. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра
7. Количественная оценка стойкости парольной защиты
8. Защита данных от несанкционированного доступа
9. Графический ключ

Выполнение лабораторных работ включает: оформление отчета к лабораторным работам, включающим краткий теоретический материал, результаты эксперимента, их анализ и представление, защита в форме собеседования по контрольным вопросам к лабораторной работе.

Перечень контрольных вопросов для защиты лабораторных работ приведен в конце каждой лабораторной работы в методических указаниях к ним.

Критерии оценивания лабораторных работ: лаб. работы, при соблюдении следующих условий (Работа выполнена полностью. Обучающийся владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, представляет полные и развернутые ответы на дополнительные вопросы. В решении нет математических ошибок). С 1 по 8 лаб. работы оцениваются по 5 баллов. 9 лаб. работа оценивается в 10 баллов.

Отчет рассматривается как критерий оценки только при выполнении обучающимся лабораторной работы. Обучающийся не допускается к защите лабораторной работы без ее выполнения и/или при отсутствии отчета.

Максимальное количество баллов, которое обучающийся может получить за проведение всех указанных в рабочей программе лабораторных работ составляет 50 баллов. Баллы учитываются в процессе проведения текущего контроля.

**Типовые практические задания к промежуточной аттестации.**

1. Дать определение системы защиты государственной тайны и укажите ее составляющие

2. Получить данные о количестве пользователей и объектов компьютерной системы

3. Выбрать идентификаторы пользователей, используемые при их входе в компьютерную систему (по одному идентификатору для каждого пользователя)

4. Реализовать программное заполнение матрицы доступа, содержащей ко¬личество пользователей и объектов

5. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов

6. Необходимо записывать зашифрованный и расшифрованный файл на диск. Должна быть обеспечена визуализация процесса шифрования и расшифрования в главном окне приложения. Метод шифрования по выбору студента из изученного материала в ходе освоения дисциплины

7. Разработать консольное приложение для генерации ключей

8. Разработать визуальное приложение для шифрования/дешифрования чисел

9. Разработать программу, реализующую привязку к компьютеру

10. Реализовать алгоритм формирования ключа и реализовать процедуры идентификации пользователей по данному ключу

Типовые практические задания оцениваются из 15 баллов исходя из критериев: отсутствие ошибок, полное решение задачи, владение теоретическим материалом, полный ответ на дополнительные вопросы.

**2.3 Типовые экзаменационные материалы**

Пример задания к промежуточной аттестации по дисциплине «*Информационная безопасность и защита информации*».



Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

### Кафедра \_\_\_\_\_\_\_\_\_\_Информационные технологии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Б И Л Е Т №\_\_1\_\_

на \_20\_ /20\_ \_ учебный год

1. Генерация простых чисел. Принципы. Алгоритмы

2. Хэш функции. Требования к хеш функциям

3. Реализовать алгоритм формирования ключа и реализовать процедуры идентификации пользователей по данному ключу

Структура оценочных материалов (оценочных средств), позволяющих оценить уровень компетенций, сформированный у обучающихся при изучении дисциплины «*Информационная безопасность и защита информации»* приведен в таблице 4.

Таблица 4 - Оценочные материалы (оценочные средства) по дисциплине «Информационная безопасность и защита информации»

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Компетенция | Знать | Оценочные средства | | Уметь | Оценочные средства | | Владеть | Оценочные средства | |
| текущий контроль | промежуточный контроль | текущий контроль | промежуточный контроль | текущий контроль | промежуточный контроль |
| ОПК-3.1 | Методы решения стандартных задач профессиональной деятельности | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Ответы на вопросы к промежуточной аттестации №1-39 | Осуществлять обмен информации с удаленными компьютерами, доступ к ресурсам Internet, поиск информации и анализ данных | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Решение заданий к промежуточной аттестации №1-10 | Методами формирования и использования баз данных и информационно-справочных систем при анализе различных данных, ресурсов телекоммуникационных технологий и глобальной сети Internet | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Решение заданий к промежуточной аттестации №1-10 |
| ОПК-3.2 | Законодательный уровень информационной безопасности, математические основы криптографии (теорию информации, понятие энтропии и неопределенности, теорию сложности, теорию чисел) | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Ответы на вопросы к промежуточной аттестации №1-39 | Разрабатывать политику информационной безопасности, проводить оценку угроз безопасности объекта информатизации, проектировать системы защиты информации | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Решение заданий к промежуточной аттестации №1-10 | Навыками программирования алгоритмов криптографической защиты информации | Ответы на вопросы к лабораторным работам №1-9. Ответы на вопросы к текущей аттестации 1 рейтинг №1-34 и 2 рейтинг №1-36 | Решение заданий к промежуточной аттестации №1-10 |