Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение   
высшего образования «Новосибирский национальный исследовательский  
государственный университет» (Новосибирский государственный университет, НГУ)

**Факультет информационных технологий**

СОГЛАСОВАНО

Декан ФИТ НГУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.М. Лаврентьев

«03» июля 2019 г.

**Фонд оценочных средств промежуточной аттестации**

**по дисциплине Криптография для информационных технологий**

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная Год обучения: 4, семестр 7

|  |  |
| --- | --- |
| Форма аттестации | Семестр |
| Экзамен | 7 |

Новосибирск 2019

**Фонд оценочных средств** промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Криптография для информационных технологий», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Программная инженерия и компьютерные науки

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 75 от 02.07.2019.

Разработчики:

Проф. кафедры компьютерных систем ФИТ,

Доктор технических наук Б.Я.Рябко

Заведующий кафедрой компьютерных систем ФИТ,

кандидат технических наук Б.Н. Пищик

доцент кафедры систем информатики ФИТ,

кандидат технических наук А.А. Романенко

1. **Содержание и порядок проведения промежуточной аттестации  
   по дисциплине**
   1. **Общая характеристика содержания промежуточной аттестации**

Промежуточная аттестация по дисциплине «Криптография для информационных технологий» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

|  |  |  |  |
| --- | --- | --- | --- |
| Код | Компетенции, формируемые в рамках дисциплины  «Введение в организацию распределенных вычислений» | Семестр 7 | |
| Портфолио | Экзамен |
| **ПКС-2** Способен разрабатывать компоненты системных программных продуктов | | | |
| **ПКС-2.3** | Уметь применять знания в области разработки ПО в предметной области | **+** | **+** |

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Устный экзамен.

Все компетенции, формируемые в рамках дисциплины, оцениваются как через портфолио, так и на устном экзамене.

Тематика контрольных работ, образующих портфолио, и экзаменационных вопросов включает следующие темы (разделы): криптография с открытым ключом, блоковые и потоковые шифры, генераторы случайных чисел и тесты для них, блокчейн и криптовалюты .

* 1. **Порядок проведения промежуточной аттестации по дисциплине**

Промежуточная аттестация проводится в форме экзамена и включает 2 этапа: портфолио и экзамен. Необходимым условием для прохождения промежуточной аттестации является оценка «зачтено» по результатам выполненного портфолио. Для оценивания портфолио студенту необходимо сдать все работы, входящие в структуру портфолио.

Экзамен проводится в устной форме. Во время проведения экзамена студенту разрешается использовать справочники, калькуляторы. В процессе ответа на вопросы экзаменационного билета студенту могут быть заданы дополнительные вопросы по темам дисциплины.

1. **Требования к структуре и содержанию фонда оценочных средств  
   промежуточной аттестации по дисциплине**

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование оценочного средства | Краткая характеристика оценочного средства | Представление оценочного средства в фонде |
| Семестр 7 | | | |
| 1 | Портфолио | Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах. | Требования к структуре и содержанию портфолио |
| 2 | Экзаменационный билет | Комплекс вопросов. | Список теоретических вопросов |

* 1. **Требования к структуре и содержанию оценочных средств  
     аттестации**

2.1.1 Требования к структуре и содержанию портфолио

Портфолио должно содержать результаты выполнения 6 домашних заданий, состоящих из решения задач.

2.1.2 Форма и перечень вопросов экзаменационного билета

**Форма  экзаменационного билета**

Таблица П1.3

|  |  |  |  |
| --- | --- | --- | --- |
|  | Новосибирский государственный университет  **Экзамен** | |  |
|  | Криптография для информационных технологий | |  |
|  | наименование дисциплины  09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА  Программная инженерия и компьютерные науки | |  |
|  | наименование образовательной программы  **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №**  1. Вопрос из категории 1  2. Вопрос из категории 2 | |  |
|  | Составитель |  |  |
|  |  | Б.Я. Рябко |  |
|  | (подпись) |  |  |
|  | Ответственный за образовательную программу | |  |
|  |  | А.А. Романенко |  |
|  | (подпись) |  |  |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20     г. |  |  |

Перечень вопросов экзамена, структурированный по категориям, представлен в таблице П1.4

Таблица П1.4

|  |  |
| --- | --- |
| Категория | Формулировка вопроса |
| ПКС-2.3  Категория 1 | Вопрос 1. Арифметика в конечных кольцах целых чисел.. |
| Вопрос 2. Алгоритмы возведения в степень. |
| Вопрос 3. Алгоритмы вычисления мультипликативной инверсии. |
| ПКС-2.3  Категория 2 | Вопрос 5. Понятие односторонней функции. |
| Вопрос 6. Система Диффи-Хеллмана в мультипликативной группе. |
| Вопрос 7. Система Диффи-Хеллмана в подгруппе простого поля |
| Вопрос 8. Шифр Эль-Гамаля в мультипликативной группе |
| Вопрос 9. Шифр Эль-Гамаля в подгруппе простого поля |
| Вопрос 10. Шифр Шамира |
| Вопрос 11. Вычисление дискретных логарифмов |
| Вопрос 12. Извлечение корней в конечных кольцах целых чисел |
| Вопрос 13. Шифр RSA |
| Вопрос 14. Цифровая подпись RSA |
| Вопрос 15. Шифр Рабина |
| Вопрос 16. Стойкость систем RSA и Рабина |
| Вопрос 17. Разложение числа на простые множители |
| Вопрос 18. Доказательства с нулевым разглашением |
| Вопрос 19. Протоколы аутентификации |
| ПКС-2.3  Категория 1 | Вопрос 20. Электронные деньги |
| Вопрос 21. Совершенные шифры |
| Вопрос 22. Идеальные и строго идеальные шифры |
| Вопрос 23. Рандомизация в криптографии |
| ПКС-2.3  Категория 2 | Вопрос 24. Защита информации на основе нумерации. |
| Вопрос 25. Омофонные коды |
| Вопрос 26. Универсальное омофонное кодирование. |

Набор экзаменационных билетов формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Криптография для информационных технологий» в текущем учебном году.

1. **Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине**

Таблица П1.5

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Шифр компетенций** | **Структурные элементы оценочных средств** | **Показатель сформированности** | **Не**  **сформирован**  **(2 балла)** | **Пороговый уровень**  **(3 балла)** | **Базовый уровень**  **(4 балла)** | **Продвинутый**  **(5 баллов)** |
| **ПКС-2.3** | Портфолио | **ПКС-2.3**  Уметь применять знания в области разработки ПО в предметной области | Фрагментарные знания | Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации, но затрудняется при их использовании | Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации, но с небольшими пробелами | Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации исленного эксперимента |
| **ПКС-2.3** | Экзамен | **ПКС-2.3**  Уметь применять знания в области разработки ПО в предметной области | Имеет фрагментарные знания методов исследования и проведения экспериментальных работ | Знать основные этапы проведения эксперимента с криптографическими методами. | Знать основные этапы проведения эксперимента с криптографическими методами. Но с пробелами. | Уметь проводить эксперименты с криптографическими методами по заданной методике и анализировать результатыУметь |

**4**. **Критерии выставления оценок по результатам промежуточной аттестации по дисциплине**

В 7 семестре результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована.

**Лист актуализации фонда оценочных средств промежуточной аттестации**

**по дисциплине  
«Криптография для информационных технологий»**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Характеристика внесенных изменений (с указанием пунктов документа) | Дата и №  протокола Ученого совета ФИТ | Подпись  ответственного |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |