МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По дисциплине

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Санкт-Петербург
2018

СОДЕРЖАНИЕ

1. Перечень компетенций и этапы их формирования в процессе освоения дисциплины.3
2. Структура ФОС по дисциплине 4
3. Показатели и критерии оценки компетенций 7
4. Шкала оценивания результата 9
5. Перечень заданий по дисциплине 9
6. Методические материалы, определяющие процедуры оценивания 13
7. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями 14

Приложение:

Контрольно-оценочные средства

1. Перечень компетенций и этапы их формирования в процессе освоения дисциплины

1.1. Фонд оценочных средств предназначен для оценки результатов обучения по учебной дисциплине.

Рабочей программой дисциплины (модуля) предусмотрено формирование следующих компетенций:

Таблица – 1.1.1. Перечень формируемых дисциплиной компетенций

Код компетенции	Наименование компетенции
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПСК-1.1	способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах

1.2. Конечными результатами освоения дисциплины являются сформированные «знать», «уметь», «владеть», расписанные по отдельным содержательным компонентом компетенций, формирующихся дисциплиной. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы. Планируемые результаты освоения дисциплины, характеризующие этапы формирования компетенции, представлены в табл. 1.2.1:

Таблица – 1.2.1. Планируемые результаты обучения по дисциплине

Этапы формирования компетенций	Наименование дисциплины	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
1	2	3
Третий уровень (продвинутый) (ОПК-7)-3	Криптографические методы защиты информации	Декомпозиция I Знать: предмет, цели и задачи криптографии и криптоанализа, принципы построения криптографических алгоритмов; криптографические стандарты, профессиональные требования к симметричным и асимметричным криптосистемам. З3 (I)(ОПК-7) Уметь: решать задачи, связанные с шифрованием и цифровой подписью сообщений; осуществлять выбор необходимых криптографических методов, алгоритмов и режимов работы криптоалгоритмов для решения практических задач информационной безопасности. У3(I) (ОПК-7) Владеть: методами имитозащиты, обеспечения конфиденциальности, аутентификации и проверки целостности с помощью криптографических алгоритмов и функций; приемами управления ключевой информацией и построения сетей засекреченной связи. В3 (I)(ОПК-7)
Третий уровень (продвинутый) (ПСК-1.1) –3	Криптографические методы защиты информации	Декомпозиция II Знать: структуру, принципы построения и основные элементы криптографических алгоритмов, криптографические алгоритмы шифрования,

		обеспечения целостности и электронной подписи З3 (II)(ПСК-1.1) Уметь: проводить анализ и построение структурных схем криптографических алгоритмов, реализовывать вычислительные алгоритмы криптографии с помощью программных инструментальных средств У3(II) (ПСК-1.1) Владеть: приемами и навыками программной реализации и анализа криптографических алгоритмов в современных программных комплексах В3 (II)(ПСК-1.1)

1.3. Входной уровень знаний, умений, опыта деятельности, требуемых для формирования компетенции:

– знает виды, возможные методы и пути реализации угроз информационной безопасности объекта защиты;

– знает методы программирования и методы разработки эффективных алгоритмов решения прикладных задач, современные средства разработки и анализа программного обеспечения на языках высокого уровня;

– знает принципы построения и анализа сложности вычислительных алгоритмов;

– умеет выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

– использует один из алгоритмических языков при решении задач;

– владеет профессиональной терминологией и навыками изучения специальной литературы по вопросам обеспечения информационной безопасности;

– владеет методами построения, количественного анализа и оценки сложности вычислительных алгоритмов;

– владеет навыками анализа и реализации алгоритмов в современных программных комплексах.

2. Структура ФОС по дисциплине

Оценка проводится методом сопоставления параметров, продемонстрированной обучающимся продукта деятельности с заданными эталонами и стандартами по критериям.

Для положительного заключения по результатам оценочной процедуры по учебной дисциплине установлено пороговое значение показателя, при котором принимается положительное решение, констатирующее результаты освоения дисциплины.

Таблица – 2.1. Объекты оценивания и наименование оценочных средств

Номер и наименование тем	**Формы текущего контроля успеваемости Формы промежуточной аттестации**	**Объекты оценивания**	**Вид занятия / Наименование оценочных средств**	**Форма проведения оценки Устная/ письменная**
1	**2**	**3**	**4**	**5**
Раздел 1. Криптосистемы с секретным ключом				
Тема 1.1.	Текущий контроль	Основные понятия и определения	Лекции,	Письменная

Основные понятия криптографии. Классические шифры		криптографии. Классические шифры замены и перестановки. Методы криптоанализа классических шифров. Формальные модели классических шифров. Расстояние единственности шифра. Идеальные криптосистемы. Теоретическая стойкость шифров.	Самостоятельная работа, ПЗ / Решение практических задач	(отчет)
Тема 1.1.		Контрольная точка №1	Индивидуальное контрольное задание №1	Письменная (отчет), устная (защита контрольного задания)
Тема 1.2. Современные симметричные блочные шифры	Текущий контроль	Совершенные и близкие к совершенным шифры. Композиции шифров. Методы синтеза симметричных блочных шифров. Сети Фейстеля. Алгоритм шифрования DES. Алгоритм «Магма» ГОСТ Р 34.12-2015. Подстановочно-перестановочные сети. Шифр AES. Алгоритм «Кузнечик» ГОСТ 34.12-2015. Режимы работы блочных шифров ГОСТ Р 34.13-2015. Специальные режимы работы блочных шифров. Практическая стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования.	Лекции, Самостоятельная работа, ПЗ / Решение практических задач	Письменная (отчет)
Тема 1.3. Потоковые системы шифрования	Текущий контроль	Потоковые криптосистемы. Генераторы ключевой гаммы на регистрах сдвига с линейной обратной связью LSFR. Нелинейные потоковые шифры. Синхронные и асинхронные потоковые шифры. Атаки на потоковые криптосистемы. Примеры потоковых криптосистем.	Лекции, Самостоятельная работа, ПЗ / Решение практических задач	Письменная (отчет)
Тема 1.4. Вопросы практической реализации симметричных криптосистем	Текущий контроль	Управление криптографическими ключами. Генераторы случайных и псевдослучайных чисел. Равномерные и неравномерные ключевые пространства. Централизованное и децентрализованное распределение ключей. Защита ключей при хранении. Имитостойкость и помехоустойчивость шифров. Программные и аппаратные шифраторы. Примеры программных реализаций средств криптографичес-кой защиты информации.	Лекции, Самостоятельная работа, ПЗ / Решение практических задач	Письменная (отчет)
Раздел 2. Криптосистемы с открытым ключом				

Тема 2.1. Асимметричная криптография	Текущий контроль	Основные концепции криптографии с открытым ключом. Система Диффи-Хеллмана. Математические основы и вычислительные алгоритмы асимметричной криптографии. Шифр Шамира. Шифр Эль-Гамаля. Атаки на криптосистемы, основанные на сложности задачи дискретного логарифмирования. Шифр RSA. Атаки на алгоритм RSA, требования к выбору параметров шифра. Криптосистема Рабина. Семантическая стойкость. Вероятностное шифрование.	Лекции, Самостоятельная работа, ПЗ/ Решение практических задач, отчет	Письменная (отчет)
Тема 2.1.		Контрольная точка №2	Индивидуальное контрольное задание №2	Письменная (отчет), устная (защита контрольного задания)
Тема 2.2. Цифровая подпись	Текущий контроль	Бесключевые функции хэширования. Функция хэширования ГОСТ Р 34.11-2012. Конструкция HMAC. Электронная подпись. Детерминированная цифровая подпись RSA. Рандомизированные цифровые подписи. Создание скрытого канала в электронной подписи.	Лекции, Самостоятельная работа, ПЗ / Решение практических задач	Письменная (отчет)
Тема 2.3. Криптография на эллиптических кривых	Текущий контроль	Основы теории эллиптических кривых. Использование эллиптических кривых в криптографии. Шифрование и криптосистема Диффи-Хеллмана на эллиптических кривых. Цифровая подпись на эллиптических кривых. Цифровая подпись ГОСТ Р 34.10-2012. Выбор параметров цифровой подписи.	Лекции, Самостоятельная работа ПЗ/ Решение практических задач	Письменная (отчет)
Тема 2.4. Квантовая криптография	Текущий контроль	Основные концепции и вопросы практической реализации квантовой криптографии	Лекции, Самостоятельная работа / Контрольный опрос	Устная (опрос)
Все разделы и темы:	**Промежуточная аттестация**	Обобщенные результаты обучения по дисциплине теоретических знаний и практических навыков	Вопросы	Устная (ответ на экзаменационный билет)
Итоговый контроль по дисциплине	**-**	Вопрос 1. Знать: Российские криптографические стандарты. Вопрос 2. Уметь: проводить анализ, выбор и реализацию криптографических алгоритмов для решения профессиональных задач. Вопрос 3. Владеть: методами шифрования, имитозащиты и цифровой подписи.	Вопросы к ГИА	**Письменная**

3. Показатели и критерии оценки компетенций

Оценка знаний, умений, владений может быть выражена в параметрах *«очень высокая», «высокая»*, соответствующая академической оценке *«отлично»; «достаточно высокая», «выше средней»,* соответствующая академической оценке *«хорошо»*; «*средняя», «ниже средней», «низкая»,* соответствующая академической оценке *«удовлетворительно»; «очень низкая»,* соответствующая академической оценке *«неудовлетворительно».*

Таблица – 3.1. Текущий контроль

№	Виды работ	Критерии оценивания			
		Отсутствует компетенция	**Базовый уровень освоения компетенции**	**Повышенный уровень освоения компетенции**	**Продвинутый уровень освоения компетенции**
1	Работа на лекциях	Отсутствие участия студента в работе на занятии	Единичное высказывание	Высказывание суждений, активное участие в работе на занятии	Высказывание неординарных суждений, активное участие в работе на занятии
2	Работа на практических/семинарских занятиях	Выполнено менее 54%	Выполнено выше 54% до 69 %	Выполнено от 70% до 84 %	Выполнено выше 85%
3	Работа на практических занятиях, решение общих практических задач	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок
4	Работа на практических занятиях, решение индивидуальных практических задач	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок

Критерии оценивания формулируются для каждой компетенции и отражают опознаваемую деятельность обучающегося, поддающуюся измерению.

Таблица – 3.2. Обобщенные критерии оценивания освоения компетенции:

1	**2 (балл 54)**	**3 (балл 55-69)**	**4 (балл 70-84)**	**5 (балл 85-100)**
Отсутствует компетенция	Отсутствует компетенция	Базовый уровень освоения компетенции	Повышенный уровень освоения компетенции	Продвинутый уровень освоения компетенции
Компетенция не освоена. Студент не владеет необходимыми знаниями.	Компетенция не освоена. Обучающийся частично показывает знания, входящие в состав компетенции, понимает их необходимость, но не может их применять.	Компетенция освоена. Обучающийся показывает общие знания, входящие в состав компетенции, имеет представление об их применении, умение извлекать и использовать основную (важную) информацию из полученных знаний	Компетенция освоена. Обучающийся показывает полноту знаний, демонстрирует умения и навыки решения типовых задач.	Компетенция освоена. Обучающийся показывает глубокие знания, демонстрирует умения и навыки решения сложных задач, умение принимать решения, создавать и применять документы, связанные с профессиональной деятельностью; способен самостоятельно решать проблему/задачу на основе изученных методов, приемов и технологий.

Базовый уровень освоения компетенций - обязательный для всех обучающихся по завершении освоения дисциплины.

Повышенный уровень освоения компетенций - превышение минимальных характеристик сформированности компетенции для обучающегося.

Продвинутый уровень освоения компетенций - максимально возможная выраженность компетенции, важен как качественный ориентир для самосовершенствования так и дополнительное к требованиям ОПОП освоение компетенций с учетом личностных характеристик:

- активное участие в конференциях, конкурсах, круглых столах и т.д. с получением зафиксированного положительного результата по вопросам, включенным в дисциплину;
- разработка и реализация проектов с применением компетенций, указанных в рабочей программе;
- демонстрирует умение применять теоретические знания для решения практических задач повышенной сложности и нестандартных задач;
- выполнение в срок всех поставленных задач.

4. Шкала оценивания результата

Таблица – 4.1. Шкала критериев оценивания компетенций

Оценка	Содержание
1 2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся**:

Формой итогового контроля по дисциплине является экзамен, итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<55	неудовлетворительно
<70	удовлетворительно
<85	хорошо
>85	отлично

5. Перечень заданий по дисциплине

5.1 Задания для текущего контроля:

Таблица - 5.1.1. Перечень заданий текущего контроля и их наименование

Наименование оценочных средств	Содержание задания
Решение практических задач	Задача 1. Криптоанализ шифров табличной перестановки Задача 2. Криптоанализ шифра простой замены Задача 3. Криптоанализ многоалфавитного шифра (шифр Виженера) Задача 4. Изучение шифра AES Задача 5. Криптоанализ блочного шифра. Слайдовая атака Задача 6. Изучение потокового шифра на LSFR Задача 7. Изучение полнодискового шифрования в ОС Windows Задача 8. Изучение шифра RSA Задача 9. Атака на алгоритм RSA методом Ферма Задача 10. Атака на алгоритм RSA методом повторного шифрования

	Задача 11. Атака на алгоритм RSA методом бесключевого чтения Задача 12. Атака на алгоритм RSA на основе Китайской теоремы об остатках Задача 13. Изучение криптосистемы Блюма – Гольдвассер Задача 14. Изучение электронной цифровой подписи Эль-Гамаля Задача 15. Создание скрытого канала в цифровой подписи Эль-Гамаля Задача 16. Вычисление точек эллиптической кривой над конечным полем Задача 17. Шифрование с использованием эллиптических кривых Задача 18. Цифровая подпись на эллиптических кривых
Контрольный опрос	Вопросы по теме Квантовая криптография 1. На каких теоретических основах строится квантовая криптография? 2. Надежность систем квантовой криптографией основана на теоретической или вычислительной стойкости? 3. Каковы проблемы практической реализации квантовых систем? 4. Каково текущее состояние реализации квантовых криптосистем? 5. Каковы основные достижения в реализации квантовых криптосистем? 6. Каков порядок расстояния, на которое может быть передано зашифрованное сообщение в квантовой криптографии? 7. Каков порядок скоростей, с которой может быть передано зашифрованное сообщение в квантовой криптографии? 8. Существуют ли коммерческие реализации квантовых шифраторов, если да, то приведите примеры.

5.2 Контрольные точки БРС

Контрольная точка №1

Индивидуальное контрольное задание №1 «Применение результатов теории К. Шеннона в криптографии»

Задание: Определить использованное с наибольшей вероятностью значение секретного ключа и соответствующий открытый текст по перехваченной криптограмме. Оценить расстояние единственности для шифра простой замены и шифра Виженера со случайным ключом.

Выполненное задание защищается преподавателю.

Методические рекомендации по подготовке:

Повторение лекционного материала, использование рекомендуемой литературы, приведенной в разделе 9.1. рабочей программы дисциплины.

Посещение консультаций преподавателя.

Процедура осуществления контроля выполнения задания осуществляется в соответствии с графиком контрольных точек и проводится по критериям.

Контрольная точка №2

Индивидуальное контрольное задание №2 «Вероятностный тест Миллера-Рабина проверки целых чисел на простоту»

Задание: Определить простоту/непростоту двух больших целых чисел с помощью теста Миллера-Рабина с вероятностью ошибки, не превышающей заданную.

Выполненное задание защищается преподавателю с оформлением отчета о проделанной работе, подготовленного с помощью текстового процессора Word. Отчет должен содержать: постановку задачи, описание шагов алгоритма тестирование с указанием числовых значений, пояснения по результатам выполнения каждого шага алгоритма, итоговый вывод о простоте/непростоте тестируемого целого числа.

Методические рекомендации по подготовке:

Повторение лекционного материала, использование рекомендуемой литературы, приведенной в разделе 9.1. рабочей программы дисциплины.

Посещение консультаций преподавателя.

Процедура осуществления контроля выполнения задания осуществляется в соответствии с графиком контрольных точек (ориентировочно 16 неделя семестра) и проводится по критериям.

5.3. Примерная тематика курсовых работ

Изучить структуру алгоритма симметричного блочного шифрования, осуществить его программную реализацию на высокоуровневом языке программирования и исследовать демонстрируемое шифром свойство лавинности.

Результатом выполнения курсовой работы являются

- теоретическое описание алгоритма шифрования, структурированный проект его реализации, основанный на принципе модульности;
- пользовательский интерфейс, позволяющий проводить шифрование и расшифровку, в том числе и для случайных входных текстов и ключей, изменять, если это допускается алгоритмом шифрования, параметры алгоритма, отображать входы и результаты заданного раунда шифрования-расшифрования, а также проводить оценку лавинного эффекта алгоритма шифрования;
- исходный текст реализации и работоспособный исполняемый программный модуль;
- наборы данных для демонстрации работы программного модуля;
- теоретические выводы по результатам анализа лавинного эффекта алгоритма шифрования;
- отчет по результатам выполнения работы.

Выполненная работа подлежит защите в процессе собеседования с преподавателем и демонстрации работы программы на компьютере, в ходе которого выясняется глубина знаний обучающегося и самостоятельность выполнения работы.

Примерные темы курсовой работы:

1. Алгоритм шифрования Blowfish
2. Алгоритм шифрования Camellia
3. Алгоритм шифрования CAST
4. Алгоритм шифрования CRYPTON
5. Алгоритм шифрования DES
6. Алгоритм шифрования FEAL
7. Алгоритм шифрования IDEA
8. Алгоритм шифрования KASUMI
9. Алгоритм шифрования Khafre, Khufu
10. Алгоритм шифрования ГОСТ Р 34.12-2015 Кузнечик
11. Алгоритм шифрования LOKI97
12. Алгоритм шифрования Lucifer
13. Алгоритм шифрования MADRYGA
14. Алгоритм шифрования ГОСТ Р 34.12-2015 Магма
15. Алгоритм шифрования MARS
16. Алгоритм шифрования Rinjdael (AES)
17. Алгоритм шифрования RC5
18. Алгоритм шифрования RC6
19. Алгоритм шифрования SAFER
20. Алгоритм шифрования Serpent
21. Алгоритм шифрования Skipjack
22. Алгоритм шифрования TEA, XTEA
23. Алгоритм шифрования Twofish
24. Алгоритм шифрования DEAL
25. Алгоритм шифрования NUSH

5.4. Промежуточная аттестация

Перечень вопросов к экзамену

1. Криптографическая система. Схема, основные понятия и принципы построения
2. Классические шифры: классификация и примеры
3. Шифры гаммирования и колонной замены
4. Алгебраическая и вероятностная модель шифра. Определение апостериорной информации о ключе, открытом тексте
5. Расстояние единственности шифра
6. Теоретическая стойкость шифров. Совершенные и близкие к совершенным шифры
7. Композиционные шифры: принципы синтеза и основные схемы
8. Алгоритм шифрования DES
9. Лавинный эффект блочных шифров
10. Режимы работы блочных шифров: простой замены (ECB) и простой замены с зацеплением (CBC)
11. Режимы работы блочных шифров: гаммирование с зацеплением (CFB)
12. Режимы работы блочных шифров: гаммирования (CTR) и гаммирование с обратной связью (OFB)
13. Режимы работы блочных шифров: полнодисковое шифрование (XTS)
14. Алгоритм "Магма" ГОСТ Р 34.12-2015 (ГОСТ 28147-89)
15. Алгоритм "Кузнечик" ГОСТ Р 34.12-2015
16. Алгоритм AES: основные характеристики и процедура шифрования
17. Алгоритм AES: процедура прямой расшифровки и процедура расширения ключа
18. Вычислительная стойкость криптоалгоритмов. Требования, предъявляемые к алгоритмам шифрования и длине ключа
19. Цели и классификация атак на алгоритмы шифрования
20. Методы криптоанализа блочных шифров: «грубой силы» и «встреча посередине»
21. Методы криптоанализа блочных шифров: линейный, дифференциальный криптоанализ и его модификации
22. Методы криптоанализа блочных шифров: слайдовая атака и атака на связанных ключах
23. Атаки на шифраторы, использующие утечки по побочным каналам
24. Потоковое шифрование, методы генерации ключевой гаммы. Синхронные и асинхронные потоковые шифры
25. Генераторы ключевой гаммы на регистрах сдвига с линейной обратной связью LSFR. Нелинейные потоковые шифры
26. Криптоанализ потоковых криптосистем
27. Потоковый шифр Salsa20
28. Управление криптографическими ключами: хранение и распределение ключей
29. Управление криптографическими ключами: генерация ключей. BBS-генератор
30. Линейные и нелинейные ключевые пространства, слабые и эквивалентные ключи, проблемы слабых процедур расширения ключа
31. Имитостойкость и помехоустойчивость шифров. Коды аутентификации MAC, HMAC
32. Типы криптосистем по ключу. Симметричные и асимметричные криптосистемы: основные принципы построения, теоретическое обоснование и свойства
33. Криптосистема Диффи-Хеллмана
34. Алгоритм быстрого возведения в степень по модулю
35. Числа, обратные по модулю. Условие существования. Расширенный алгоритм Евклида, вычисление числа, обратного по модулю
36. Алгоритмы проверки чисел на простоту
37. Шифр Шамира
38. Шифр Эль-Гамаля

39. Криптосистема RSA: теоретическое обоснование, обеспечение конфиденциальности и аутентичности сообщений
40. Требования к параметрам и атаки на шифр RSA
41. Понятие семантической стойкости. Система вероятностного шифрования Блюма-Гольдвассер
42. Бесключевые хэш-функции. Стандарты и принципы построения
43. Функция хэширования ГОСТ Р 34.11-2012
44. Электронная подпись: свойства, детерминированные и вероятностные подписи. Система электронной подписи RSA
45. Система электронной подписи Эль-Гамаля
46. Система электронной подписи Шнорра
47. Эллиптические кривые: определение, вид, уравнение, операции с точками
48. Эллиптические кривые: применение в криптографии, аналог схемы Диффи-Хэллмана на эллиптических кривых, требования к параметрам кривой
49. Стандарт цифровой подписи ГОСТ Р 34.10-2012, выбор параметров кривой, подписание сообщений и проверка подписи
50. Основные принципы и проблемы практической реализации квантовой криптографии

6. Методические материалы, определяющие процедуры оценивания

Процедура оценивания результатов обучения по дисциплине характеризующих этапы формирования компетенции, представлена паспортом фонда оценочных средств по дисциплине (раздел 1).

Комплект оценочных средств хранится на кафедре, ежегодно обновляется. Для промежуточной аттестации в виде экзамена КОС по дисциплине обновляется и утверждается за 14 дней до начала сессионного периода и хранится в недоступном месте от несанкционированного доступа. Ответственность несет кафедра.

Порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся Университета по ОПОП регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования.

Текущий контроль успеваемости в Университете является формой контроля качества знаний обучающихся, осуществляемого в межсессионный период обучения с целью определения качества освоения ОПОП.

Текущий контроль успеваемости осуществляется: на лекциях, практических (семинарских) занятиях, в рамках контроля самостоятельной работы.

Обучающиеся заранее информируются о критериях и процедуре текущего контроля успеваемости преподавателями по соответствующей учебной дисциплине (модуля).

Успеваемость при текущем контроле характеризует объем и качество выполненной обучающимся работы по дисциплине (модулю).

Педагогические виды и формы, используемые в процессе текущего контроля успеваемости обучающихся, определяются методической комиссией кафедры. Выбираемый вид текущего контроля обеспечивает наиболее полный и объективный контроль (измерение и фиксирование) уровня освоения результатов обучения по дисциплине.

Преподаватели предоставляют сведения о текущей успеваемости обучающихся в рамках проведения текущей аттестации в семестре в деканаты/ учебный отдел института в сроки, определенные внутренними распорядительными документами Университета (факультета, *института*).

В целях обеспечения текущего контроля успеваемости преподаватель проводит консультации.

Преподаватель, ведущий занятия семинарского типа, проводит **аттестацию обучающихся за прошедший период**. Аттестация проводится, если проведено не менее 3 практических (семинарских) или лабораторных занятий, в установленные деканатом/институтом сроки, не реже 1 раза за учебный семестр. Обучающиеся аттестуются путем выставления в соответствующую групповую ведомость записей по системе: «аттестован» или «не аттестован».

Преподаватель, проставляя итоги аттестации, доводит результаты аттестации до сведения студенческой группы и объясняет причины отрицательной аттестации по запросу обучающегося.

При аттестации обучающихся учитываются следующие факторы:

– результаты работы на занятиях, показанные при этом знания по дисциплине (модулю), усвоение навыков практического применения теоретических знаний, степень активности на практических (семинарских) занятиях;

– результаты и активность участия в семинарах и коллоквиумах;

– результаты выполнения контрольных работ;

– результаты и объем выполненных заданий в рамках самостоятельной работы обучающихся;

– результаты личных бесед со студентами по материалу учебной дисциплины (модуля);

– посещение студентами, семинарских и практических занятий, лабораторных работ;

– своевременная ликвидация задолженностей по пройденному материалу, возникших вследствие пропуска занятий либо неудовлетворительных оценок по результатам работы на занятиях.

– результаты прохождения контрольных точек по дисциплине (при использовании балльно-рейтинговой системы)

Промежуточная аттестация обучающихся Университета является формой контроля результатов обучения по дисциплине с целью комплексного определения соответствия уровня и качества знаний, умений и навыков обучающихся требованиям, установленным образовательной программой.

Формирование оценки текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины осуществляется с использованием балльно-рейтинговой системы оценки знаний обучающихся, требования к которым изложены в Положении о балльно-рейтинговой системе.

7. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями

Адаптированные оценочные материалы содержатся в адаптированной ОПОП. Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

Самостоятельная работа обучающихся с ограниченными возможностями здоровья и инвалидов позволяет своевременно выявить затруднения и отставание и внести коррективы в учебную деятельность. Конкретные формы и виды самостоятельной работы обучающихся лиц с ограниченными возможностями здоровья и инвалидов устанавливаются преподавателем. Выбор форм и видов самостоятельной работы, обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с

учетом их способностей, особенностей восприятия и готовности к освоению учебного материала. Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере, в форме тестирования, электронных тренажеров и т.п.).

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа. Для обучающихся с нарушениями зрения предусматривается возможность проведения текущего и промежуточного контроля в устной форме. Для обучающихся с нарушениями слуха предусматривается возможность проведения текущего и промежуточного контроля в письменной форме.

Таблица 7.1. – Категории обучающихся с ОВЗ, способы восприятия ими информации и методы их обучения.

<table>
<tr><th colspan="2">Категории обучающихся по нозологиям</th><th>Методы обучения</th></tr>
<tr><td rowspan="2">С нарушениями зрения</td><td>Слепые. Способ восприятия информации: осязательно-слуховой</td><td rowspan="2">Аудиально-кинестетические, предусматривающие поступление учебной информации посредством слуха и осязания.
Могут использоваться при условии, что визуальная информация будет адаптирована для лиц с нарушениями зрения:
визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания;
аудио-визуальные, основанные на представление учебной информации, при которых задействовано зрительное и слуховое восприятие;
аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.</td></tr>
<tr><td>Слабовидящие. Способ восприятия информации: зрительно-осязательно-слуховой</td></tr>
<tr><td rowspan="2">С нарушениями слуха</td><td>Глухие. Способ восприятия информации: зрительно-осязательный</td><td rowspan="2">визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания.
Могут использоваться при условии, что аудиальная информация будет адаптирована для лиц с нарушениями слуха:
аудио-визуальные, основанные на представление учебной информации, при которых задействовано зрительное и слуховое восприятие;
аудиально-кинестетические, предусматривающие поступление учебной информации посредством слуха и осязания;
аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.</td></tr>
<tr><td>Слабослышащие. Способ восприятия информации: Зрительно-осязательно-слуховой</td></tr>
<tr><td>С нарушениями опорно-двигательного аппарата</td><td>Способ восприятия информации: зрительно-осязательно-слуховой</td><td>– визуально-кинестетические;
– аудио-визуальные;
– аудиально-кинестетические;
– аудио-визуально-кинестетические.</td></tr>
</table>

Таблица 7.2. – Способы адаптации образовательных ресурсов.

Условные обозначения:

«+» —образовательный ресурс, не требующий адаптации;

«АФ» — адаптированный формат к особенностям приема-передачи информации обучающихся инвалидов и лиц с ОВЗ формат образовательного ресурса, в том числе с использованием специальных технических средств;

«АЭ»— альтернативный эквивалент используемого ресурса

Категории обучающихся по нозологиям		**Образовательные ресурсы**				
		Электронные				**Печатные**
		мультимедиа	**графические**	**аудио**	**текстовые, электронные аналоги печатных изданий**	
С нарушениями зрения	Слепые	АФ	АЭ (например, создание материальной модели графического объекта (3Dмодели)	+	АЭ (например, аудио описание)	АЭ (например, печатный материал, выполненный рельефно-точечным шрифтом Л.Брайля)
	Слабовидящие	АФ	АФ	+	АФ	АФ
С нарушениями слуха	Глухие	АФ	+	АЭ (например, текстовое описание, гипер-ссылки)	+	+
	Слабослышащие	АФ	+	АФ	+	+
С нарушениями опорно-двигательного аппарата		+	+	+	+	+

Таблица 7.3. - Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ в СПбГЭУ

Категории обучающихся по нозологиям	**Форма контроля и оценки результатов обучения**
С нарушениями зрения	– *устная проверка:* дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – *с использованием компьютера и специального ПО*: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.
С нарушениями слуха	– *письменная проверка:* контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – *с использованием компьютера и специального ПО:* работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.

С нарушениями опорно-двигательного аппарата	– *письменная проверка, с использованием специальных технических средств* (альтернативных средства ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – *устная проверка, с использованием специальных технических средств* (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – *с использованием компьютера и специального ПО* (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы - предпочтительнее обучающимся, ограниченным в передвижении и др.

7.1. Задания для текущего контроля для инвалидов и лиц с ограниченными возможностями

Текущий контроль и промежуточная аттестация обучающихся инвалидов и лиц с ОВЗ осуществляется с использованием оценочных средств, адаптированных к ограничениям их здоровья и восприятия информации, в том числе с использованием специальных технических средств.

Текущий контроль успеваемости для обучающихся инвалидов и лиц с ОВЗ направлен на своевременное выявление затруднений и отставания в обучении и внесения коррективов в учебную деятельность. Возможно осуществление входного контроля для определении его способностей, особенностей восприятия и готовности к освоению учебного материала.

7.2. Задания для промежуточной аттестации для инвалидов и лиц с ограниченными возможностями

Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа.

Промежуточная аттестация, при необходимости, может проводиться в несколько этапов. Для этого рекомендуется использовать рубежный контроль, который является контрольной точкой по завершению изучения раздела или темы дисциплины, междисциплинарного курса, практик и ее разделов с целью оценивания уровня освоения программного материала. Формы и срок проведения рубежного контроля определяются преподавателем (мастером производственного обучения) с учетом индивидуальных психофизических особенностей обучающихся.