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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По дисциплине

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

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 6
4. Шкала оценивания результата 8
5. Перечень заданий по дисциплине 9
6. Методические материалы, определяющие процедуры оценивания 12
7. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями 13

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
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

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
Второй уровень (углубленный) (ПК-1) –2	Криптографические протоколы	Декомпозиция I Знать: принципы построения криптографических протоколов и способы их реализации в компьютерных системах, назначение, функции и принципы построения средств криптографической защиты информации З2 (I)(ПК-1) Уметь: применять средства криптографической защиты информации для решения профессиональных задач У2(I) (ПК-1) Владеть: навыками установки, настройки и администрирования средств криптографической защиты информации В2 (I)(ПК-1)
Первый уровень (пороговый) (ПК-4) –1	Криптографические протоколы	Декомпозиция III Знать: области применения и назначение криптографических протоколов, основные протоколы аутентификации, выработки ключей, обеспечения целостности и конфиденциальности З1 (III)(ПК-4) Уметь: производить выбор криптографических протоколов и настройку параметров криптографии в системах криптографической защиты информации У1(III) (ПК-4) Владеть: навыками использования криптографических методов и средств для реализации требований политики безопасности В1 (III)(ПК-4)

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 предмет, цели и задачи криптографии и криптоанализа, принципы построения криптографических алгоритмов; криптографические стандарты, профессиональные требования к симметричным и асимметричным криптосистемам;

– знает структуру, принципы построения и основные элементы криптографических алгоритмов, криптографические алгоритмы шифрования, обеспечения целостности и электронной подписи;

– решает задачи, связанные с шифрованием и цифровой подписью сообщений; осуществляет выбор необходимых криптографических методов, алгоритмов и режимов работы криптоалгоритмов для решения практических задач информационной безопасности;

– реализовывает вычислительные алгоритмы криптографии с помощью программных инструментальных средств;

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

– владеет методами анализа угроз согласно требованиям руководящих документов;

– владеет методами имитозащиты, обеспечения конфиденциальности, аутентификации и проверки целостности с помощью криптографических алгоритмов и функций; приемами управления ключевой информацией и построения сетей засекреченной связи;

– владеет приемами и навыками программной реализации и анализа криптографических 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. Основные криптографические протоколы и методы реализации				
Тема 1.1. Основы теории криптографичес-ких протоколов	Текущий контроль	Криптографические примитивы и криптографические протоколы. Виды криптографических протоколов. Формальное описание протокола. Компрометация протокола. Виды атак на криптографические протоколы. Методы анализа протоколов. Основные подходы к конструированию	Лекции, Самостоятельная работа / Контрольный опрос	Устная (опрос)

		безопасных протоколов.		
Тема 1.1.		Контрольная точка №1	Индивидуальное контрольное задание	Письменная (отчет) устная (защита контрольного задания)
Тема 1.2. Выработка криптографического ключа на основе пароля	Текущий контроль	Проблема подбора пароля. Алгоритм выработки ключа из пароля в приложениях. Функции диверсификации ключа PBKDF2, scrypt. Контроль целостности PBMAC1 и шифрование PBEC2. Практические реализации парольной защиты ключевой информации.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	Устная (опрос) Письменная (отчет)
Тема 1.3. Протоколы аутентификации	Текущий контроль	Простейшие протоколы односторонней аутентификации с предраспределенным ключом. Парольная аутентификция. Схемы аутентификации вида «запрос - ответ». Схемы аутентификации для мобильных устройств. Интерактивные системы доказательств с нулевым разглашением. Аутентификация с нулевым разглашением. Методы анализа схем аутентификации.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	Устная (опрос) Письменная (отчет)
Тема 1.4. Распределение открытых ключей	Текущий контроль	Проблема компрометации открытого ключа при передаче. Цифровые сертификаты. Модели доверия на основе цепей сертификации. Инфраструктура открытых ключей PKI.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	Устная (опрос) Письменная (отчет)
Тема 1.5. Распределение и согласование секретных ключей	Текущий контроль	Свойства протоколов распределения ключей. Предварительное распределение ключей. Схема Блома. Протокол выработки общего ключа с аутентификацией на основе пароля. Протоколы распределения ключей с доверенным центром, основанные на симметричных криптосистемах. Протокол Kerberos. Расширение протокола Kerberos PKINIT для использования криптографии с открытым ключом. Протокол Диффи-Хэллмана формирования общего секретного ключа и его обобщения. Протоколы MTI и STS. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. Протокол Нидхема-Шредера. Протоколы обновления сеансовых ключей.Методы анализа протоколов распределения ключей.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	Устная (опрос) Письменная (отчет)
Тема 1.6.	Текущий	Понятие безопасности протокола.	Лекции,	Устная

Защищенные сетевые протоколы	контроль	Функции-сервисы безопасности. Протоколы каналов защищенной передачи данных PPTP, L2TP, IPSec, SSL/TLS, SHH. Алгоритмы, используемые защищенными сетевыми протоколами: согласование ключей VKO, алгоритм диверсификации KDF, псевдослучайные функции на основе конструкции HMAC (в протоколах TLS, IPSec), экспорт и импорт ключей. Шифрование в мессенджерах.	Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	(опрос) Письменная (отчет)
Раздел 2. Специальные применения криптографических протоколов				
Тема 2.1. Специальные схемы цифровой подписи и протоколы финансовой криптографии	Текущий контроль	Цифровая подпись с восстановлением сообщения. Протокол подписи с ограниченным жизненным циклом. Схема подписи с верификацией по запросу (Казаринов). Групповая цифровая подпись. Пороговая цифровая подпись. Слепая цифровая подпись и ее применения. Системы электронных платежей и электронные деньги. Электронные банкноты Шаума. Децентрализованные системы электронных платежей. Криптовалюты. Технология блокчейн.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос, Решение практических задач	Устная (опрос) Письменная (отчет)
Темы 1.3 – 1.6, Тема 2.1		Контрольная точка №2	Исследование (эссе)	Письменная (эссе) устная (презентация)
Тема 2.2. Разделение секрета	Текущий контроль	Основные понятия и простейшие схемы разделения секрета. Пороговые схемы разделения секрета. Совершенность и идеальность схемы разделения секрета. Проверяемое разделение секрета. Протокол конфиденциальных вычислений.	Лекции, Самостоятельная работа, ПЗ / Контрольный опрос	Устная (опрос)
Все темы:	**Промежуточная аттестация**	Обобщенные результаты обучения по дисциплине теоретических знаний и практических навыков	Вопросы	**Устная**
Итоговый контроль по дисциплине	-	Вопрос 1. Знать: основные протоколы обеспечения конфиденциальности, целостности, аутентификации, распределения и согласования ключей. Вопрос 2. Уметь: проводить анализ, выбор и настройку параметров криптографических протоколов для решения профессиональных задач. Вопрос 3. Владеть: навыками установки, настройки и администрирования средств криптографической защиты информации.	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	Компетенция освоена. Обучающийся показывает общие знания, входящие в состав компетенции, имеет представление об их применении, умение извлекать и	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

	необходимость, но не может их применять.	использовать основную (важную) информацию из полученных знаний		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

Оценка	Содержание
	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 дифференцированный зачет (зачет с оценкой), 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. Изучение криптографических средств ОС Linux Задача 2. Изучение схем аутентификации с нулевым разглашением Задача 3. Развертывание PKI инфраструктуры в корпоративной сети Задача 4. RSA-сертификаты. Статическая аутентификация данных Задача 5. RSA-сертификаты. Динамическая аутентификация данных Задача 6. RSA-сертификаты. Комбинированная динамическая аутентификация данных и выработка криптограммы Задача 7. Настройка Kerberos аутентификации в корпоративной сети Задача 8. Работа с пакетом криптографических функций OpenSSL в режиме командной строки Задача 9. Изучение системы электронных денег Чаума Задача 10. Изучение технологии блокчейн Задача 11. Изучение пороговой схемы Шамира разделения секрета
Контрольный опрос	1. Понятие криптографического протокола. Иерархическое построение криптографических протоколов. Виды криптографических протоколов. 2. Формальное описание протокола. 3. Компрометация протокола. Виды уязвимостей и атак на криптографические протоколы. 4. Методы анализа криптографических протоколов. 5. Подходы к конструированию безопасных криптографических протоколов. 6. Шифрование на основе значения пароля. Проблема подбора пароля и пути ее решения. 7. Алгоритм выработки ключа из пароля в приложениях MS Office. 8. Функция диверсификации ключа PBKDF2 9. Функция диверсификации ключа scrypt. 10. Алгоритмы контроля целостности PBMAC1 и шифрования PBEC2.

	11. Протоколы аутентификации: области применения, виды и методы анализа. 12. Парольная аутентификция, ее виды и методы повышения надежности. 13. Схемы аутентификации вида «запрос - ответ». 14. Схемы аутентификации для мобильных устройств. 15. Интерактивные системы доказательств с нулевым разглашением – основные концепции и свойства. 16. Система доказательств, основанная на задаче об изоморфизме графов. 17. Аутентификация с нулевым разглашением. Схемы аутентификации Фиата – Шамира и Файге – Фиата – Шамира. 18. Схемы аутентификации Шнорра и Брикелла – МакКарли. Протокол идентификации Окамото. 19. Протокол идентификации Гиллу-Кискате. 20. Проблема компрометации открытого ключа при передаче, атаки на открытые ключи и методы противодействия. 21. Цифровые сертификаты. Модели доверия на основе цепей сертификации. 22. Инфраструктура открытых ключей PKI. 23. Протоколы распределения и согласования ключей: области применения, виды и методы анализа. 24. Предварительное распределение ключей. Схема Блома. 25. Протокол выработки общего ключа с аутентификацией на основе пароля. 26. Протоколы распределения ключей с доверенным центром, основанные на симметричных криптосистемах. 27. Протокол Kerberos. Расширение протокола Kerberos PKINIT для использования криптографии с открытым ключом. 28. Протокол Диффи-Хэллмана. Протоколы MTI и STS. Возможные атаки на протоколы и пути противодействия. 29. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. Протокол Нидхема-Шредера. 30. Протоколы обновления сеансовых ключей. 31. Понятие безопасности протокола. Функции-сервисы безопасности. 32. Протоколы каналов защищенной передачи данных. 33. Алгоритм согласования ключей VKO. 34. Алгоритм диверсификации KDF. 35. Псевдослучайные функции на основе конструкции HMAC, алгоритмы экспорта и импорта ключей. 36. Криптографическая защита информации в мессенджерах. 37. Цифровая подпись с восстановлением сообщения. 38. Протокол подписи с ограниченным жизненным циклом. 39. Схема подписи с верификацией по запросу. 40. Групповая цифровая подпись. 41. Пороговая цифровая подпись. 42. Слепая цифровая подпись: области применения, свойства и варианты алгоритмов. 43. Системы электронных платежей и электронные деньги. Электронные банкноты Чаума. 44. Децентрализованные системы электронных платежей. Криптовалюты. Технология блокчейн. 45. Основные понятия и простейшие схемы разделения секрета. Совершенность и идеальность схемы разделения секрета. Проверяемое разделение секрета. 46. Пороговая схема разделения секрета Блекли. 47. Пороговая схема разделения секрета Шамира. 48. Пороговая схема разделения секрета на основе Китайской теоремы об остатках.

	49. Разделение секрета для произвольной структуры доступа. Протоколы конфиденциальных вычислений.

5.2 Контрольные точки БРС

Контрольная точка 1

Индивидуальное контрольное задание «Разработка протокола»

Задание: Разработать протокол, нацеленный на решение конкретной задачи, определенной преподавателем.

Выполненное задание защищается преподавателю с оформлением отчета о проделанной работе, подготовленного с помощью текстового процессора Word. Отчет о выполнении задания должен содержать описание действующих сторон (ролей) и шагов протокола; анализ возможности проведения атак на протокол (следует рассмотреть все типовые атаки), анализ возможности мошенничества со стороны участников протокола.

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

Исследование (эссе) «Исследование криптографических протоколов и примитивов, реализованных в защищенной информационной системе»

Задание: Исследовать подсистему криптографической защиты информации общеизвестной защищенной информационной системы (по согласованию с преподавателем). Примерами подобных систем могут быть операционные системы, сетевые клиент-серверные приложения, утилиты, реализующие высокоуровневые сетевые протоколы, отдельные средства защиты информации.

Выполненное задание защищается преподавателю с оформлением отчета о проделанной работе, подготовленного с помощью текстового процессора Word. Отчет должен содержать: постановку задачи, общее описание информационной системы и функций безопасности, использующих подсистему криптографической защиты информации; описание структуры подсистемы криптографической защиты, реализованные в системе сетевые протоколы и конкретные задачи, которые решаются с их помощью (например: сетевая одностороння аутентификация пользователей web-ъшгашге – протокол TLS); криптографические протоколы, используемые высокоуровневым сетевым протоколом (например: TLS – протокол аутентификации с согласованием ключей VKO, алгоритм диверсификации KDF, псевдослучайные функции на основе конструкции HMAC) с кратким описанием каждого криптографического протокола; реализованные криптографические алгоритмы (например: шифрование – ГОСТ Р 34.12-2015 Магма) с указанием конкретных параметров криптографических алгоритмов, если поддерживается несколько вариантов алгоритма (например, AES-128 – алгоритм AES с 128-битным ключом); общий вывод о степени безопасности системы при использовании различных настроек криптографии (если поддерживаются).

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.

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.

Категории обучающихся по нозологиям		Методы обучения
С нарушениями зрения	Слепые. Способ восприятия информации: осязательно-слуховой	*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
	Слабовидящие. Способ	

	восприятия информации: зрительно-осязательно-слуховой	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.
С нарушениями слуха	Глухие. Способ восприятия информации: зрительно-осязательный Слабослышащие. Способ восприятия информации: Зрительно-осязательно-слуховой	*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.
С нарушениями опорно-двигательного аппарата	Способ восприятия информации: зрительно-осязательно-слуховой	– *визуально-кинестетические*; – *аудио-визуальные*; – *аудиально-кинестетические*; – *аудио-визуально-кинестетические.*

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 нарушениям и слуха	Глухие	АФ	+	АЭ (например, текстовое описание, гипер-ссылки)	+	+
	Слабослышащ ие	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.