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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По дисциплине

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА 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.....8
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
Второй уровень (углубленный) (ОПК-7)-2	Программно-аппаратные средства защиты информации	Декомпозиция II Знать: методы и средства защиты информации; - возможности современных программно-аппаратных средств защиты информации З2 (II)(ОПК-7) Уметь: на основе полученных знаний самостоятельно осуществлять выбор, установку и настройку программно-аппаратных средств защиты информации, исходя из условий поставленной задачи У2(II) (ОПК-7) Владеть: методами выбора, установки и настройки программно-аппаратных средств защиты информации, исходя из условий поставленной задачи В2 (II)(ОПК-7)
Третий уровень (продвинутый) (ПСК-1.1) –3	Программно-аппаратные средства защиты информации	Декомпозиция I Знать: программно-аппаратные средства и методы защиты информации в операционных системах; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации З3 (I)(ПСК-1.1) Уметь: производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации; осуществлять мероприятия по

		противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения; определять порядок функционирования программного обеспечения с целью обеспечения защиты информации. У3(I) (ПСК-1.1) Владеть: конфигурированием программно-аппаратных средств защиты информации в операционных системах; формированием шаблонов установки программно-аппаратных средств защиты информации в операционных системах; формулированием требований к встроенным средствам защиты информации программного обеспечения. В3 (I)(ПСК-1.1)

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

- формулирует основные определения информатики;
- выполняет решения задач с использованием стандартных алгоритмов;
- использует современные технические средства на уровне пользователя;
- использует один из алгоритмических языков при решении задач.

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**
Тема 1. Предмет и задачи программно-аппаратной защиты информации	Текущий контроль	Классификация задач программно-аппаратной защиты информации	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная
Тема 2. Основные понятия	Текущий контроль	Основные понятия программно-аппаратной защиты информации	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 3. Понятие уязвимости компьютерных систем	Текущий контроль	Понятие уязвимости компьютерных систем	Лекции/Самостоятельная работа/Контрольный опрос	Устная

Тема 4. Политика безопасности в компьютерных системах. Оценка защищенности	Текущий контроль	Политика безопасности в компьютерных системах.	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная
Тема 5. Понятие идентификации пользователя	Текущий контроль	Понятие идентификации пользователя	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 6. Основные подходы к защите данных от НСД	Текущий контроль	Основные подходы к защите данных от НСД	Лекции/Самостоятельная работа/Контрольный опрос	Устная
Тема 7. Организация доступа к файлам	Текущий контроль	Организация доступа к файлам	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная
Тема 7.		Контрольная точка 1	Индивидуальное задание 1	Письменная
Тема 8. Фиксация доступа к файлам	Текущий контроль	Фиксация доступа к файлам в ОС	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 9. Доступ к данным со стороны процесса	Текущий контроль	Доступ к данным со стороны процесса	Лекции/Самостоятельная работа/Контрольный опрос	Устная
Тема 10. Особенности защиты данных от изменения	Текущий контроль	Методы защиты данных от изменения	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная
Тема 11. Построение программно-аппаратных комплексов шифрования	Текущий контроль	Программно-аппаратные комплексы шифрования	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 12. Компоненты ПЭВМ	Текущий контроль	Компоненты ПЭВМ	Лекции/Самостоятельная работа/Контрольный опрос	Устная
Тема 13. Проблема защиты отчуждаемых компонентов ПЭВМ	Текущий контроль	Защита отчуждаемых компонентов ПЭВМ	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная

Тема 14. Надежность средств защиты компонент	Текущий контроль	Надежность средств защиты компонент	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 15. Несанкционированное копирование программ	Текущий контроль	Несанкционированное копирование программ	Лекции/Самостоятельная работа/Контрольный опрос	Устная
Тема 16. Подходы к задаче защиты от копирования	Текущий контроль	Методы защиты от копирования	Лекции/Лабораторные работы/Самостоятельная работа/Решение практических задач	Письменная
Тема 16.		Контрольная точка 2	Индивидуальное задание 2	Письменная
Тема 17. Пароли и ключи	Текущий контроль	Пароли и ключи	Лекции/Практическое занятие/Контрольный опрос	Устная
Тема 18. Организация хранения ключей (с примерами реализации)	Текущий контроль	Организация хранения ключей (с примерами реализации)	Лекции/Самостоятельная работа/Контрольный опрос	Устная
Тема 19. Типовые решения в организации ключевых систем	Текущий контроль	Типовые решения в организации ключевых систем	Лекции/Лабораторные работы/Решение практических задач	Письменная
Тема 20. Изучение и обратное проектирование ПО	Текущий контроль	Изучение и обратное проектирование ПО	Лекции/Практическое занятие/Самостоятельная работа/Контрольный опрос	Устная
Тема 20.		Контрольная точка 2	Индивидуальное задание 3	Письменная
Тема 21. Задачи защиты от изучения и способы их решения	Текущий контроль	Задачи защиты от изучения и способы их решения	Лекции/Контрольный опрос	Устная
Тема 22. Аспекты проблемы защиты от исследования	Текущий контроль	Аспекты проблемы защиты от исследования	Лабораторные работы/Решение практических задач	Письменная
Тема 23. Компьютерные вирусы	Текущий контроль	Компьютерные вирусы	Практическое занятие/ Контрольный опрос	Устная
Все темы и разделы:	**Промежуточная аттестация**	Обобщенные результаты обучения по дисциплине теоретических знаний и практических навыков	Вопросы	**Устная**

Итоговый контроль по дисциплине	-	Вопрос 1. Современное состояние и тенденции в области защиты информации от несанкционированного доступа. Вопрос 2. Методы защиты информации от несанкционированного доступа.	Вопросы к ГИА	-

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	Разработка программы разграничения полномочий пользователей на основе парольной аутентификации Привязка ПО к аппаратному окружению и физическим носителям как средство защиты от копирования ПО Разработка и программная реализация криптографических алгоритмов Организация доступа к файлам в различных ОС Использование функций криптографического интерфейса Windows для защиты информации Исследование системы обнаружения вторжений Защита программного обеспечения от несанкционированного использования и копирования Исследование методов защиты от дизассемблирования ПО Основы работы с персональным межсетевым экраном фирмы «Инфотекс» Основы работы с комплексом СЗИ от НСД от фирмы «Код безопасности»

5.2 Контрольные точки БРС

Контрольная точка 1

Индивидуальное задание 1. Исследование методов защиты от дизассемблирования ПО.

Выполненный проект 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 задание 2. Основы работы с персональным межсетевым экраном фирмы «Инфотекс»

Выполненный проект защищается преподавателю, после чего оформляется в Word отчет о проделанной работе, который должен содержать: постановку задачи, вид всех используемых в проекте форм, описание элементов управления в формах, программный текст процедур и отправляется преподавателю на почту.

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.

Индивидуальное задание 3. Основы работы с комплексом СЗИ от НСД от фирмы «Код безопасности».

Выполненный проект защищается преподавателю, после чего оформляется в Word отчет о проделанной работе, который должен содержать: постановку задачи, вид всех используемых в проекте форм, описание элементов управления в формах, программный текст процедур и отправляется преподавателю на почту.

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.

5.3. Примерная тематика курсовых работ

Варианты тем курсовых работ:

1. Расследование компьютерных преступлений.
2. Создание программного комплекса для тестирования на проникновение
3. беспроводных сетей.
4. Эмуляция работы стресс-тестов сети.
5. Анализ уязвимостей в веб-приложениях.
6. Анализ уязвимостей в операционных системах и серверном программном
7. обеспечении.

8. Создание стенда для демонстрации сканирование сетей. Перехват данных в сетях.
9. Анализ сетевого трафика.
10. Создание программного комплекса по моделированию атак на пароли.
11. Разработка персонального помощника для администратора безопасности.
12. Структуризация знаний в области защиты информации (построение онтологии).
13. Разработка архитектуры защищенной системы обнаружения вторжений.
14. Создание программного комплекса по моделированию атак на веб-сервер.
15. Разработка архитектуры системы комплексного сетевого сканирования
16. защищенности.
17. Система сбора данных журналов регистрации событий операционных систем.
18. Эмуляция работы защищенных сетевых протоколов.
19. Эмуляция конкретных видов атак.
20. Создание интерфейсов для эмуляции работы средств защиты.
21. Изучение зависимости между топологией сети и атаками.
22. Изучение атак на сетевое аппаратное обеспечение.
23. Изучение сетевых сканеров уязвимостей.
24. Изучение атак на приложения и защита приложений.
25. Исследование защитных сервисов - тесты на возможность проникновения.
26. Мандатный и ролевой доступ в Linux. GRSecurity, SELinux, RBAC в некоторых
27. файловых системах.
28. Криптоанализ. Простейший частотный анализ, атаки на криптографические
29. протоколы.
30. Применение криптографии в сетях. SSL/TLS, ЭЦП, протоколы аутентификации,
31. управление доверием. Примеры атак – перебор по словарю, rainbow таблицы.
32. Протоколы PGP и S/MIME и их реализации.

5.4. Промежуточная аттестация

Вопросы к экзамену:

1. Электронные ключи Guardant. Электронный ключ Guardant Sign. Электронный ключ Guardant Code. Лицензирование сетевых приложений. Защищенные схемы продаж.
2. Электронные ключи Guardant. Guardant SP. Сервер активации. Принцип работы. Технические характеристики.
3. Электронные ключи Guardant. Выбор модели ключа. Защита Windows-приложений.
4. Электронные ключи Guardant. Выбор модели ключа. Удаленное обновление памяти ключа.
5. Комплекты разработчика Guardant. Выбор модели ключа.
6. Электронный идентификатор Rutoken. Комплект разработчика Rutoken
7. Комплект разработчика Rutoken. Электронные идентификаторы Рутокен Web.
8. Назначение ПО VipNet Custom. Файл дистрибутив (VipNet Custom)
9. Состав программного комплекса ViPNet. Криптоядро Домен-К.
10. Логика обработки IP-трафика VipNet
11. Аппаратные ключи защиты серии HASP. Аппаратные ключи защиты HASP 4-го и 5-го поколения.
12. ViPNet Custom. Файл-дистрибутив VipNet. dst, КД и КН файлы.
13. Ключ Guardant: назначение, основные характеристики, пример использования
14. ViPNet Administrator (Администратор). Особенности ключевой структуры VipNet.
15. Аппаратные ключи защиты RuToken
16. VipNet Custom. Особенности взаимодействия ЦУС и УКЦ. Сетевые экраны: назначение, примеры использования.
17. Аппаратные ключи защиты eToken
18. Виртуальные защищенные сети: виды, характеристики и варианты реализации.

19. Ключ eToken: назначение, основные характеристики, пример использования
20. Режимы работы ViPNet Driver. Фильтрация, критерии и правила. Виды фильтров.
21. Ключ ruToken: назначение, основные характеристики, пример использования
22. Аппаратные ключи защиты серий HASP SRM (HL, SL) и HASP 4. Сравнительные характеристики, область применения.
23. Ключевой и удостоверяющий центр VipNet Custom. Технология разграничения доступа к информации на примере ViPNet
24. Межсетевые экраны. ДМЗ (на примерах VipNet Custom). Создание виртуальной защищенной сети VipNet
25. Понятие адресной и прикладной администрации в ViPNet. Клиентское программное обеспечение для организации защищенной сети ViPNet Client (Клиент).
26. Логика использования виртуальных адресов в ViPNet Custom. Компоненты ViPNet Custom. ViPNet [Координатор]: назначение, особенности.
27. VipNet Custom. ЦУС и УКЦ, особенности взаимодействия. Криптоядро «Домен-К»
28. VipNet Custom. Межсетевое взаимодействие. Виды ММК в VipNet. Серверное программное обеспечение для организации защищенной сети ViPNet Coordinator (Координатор)
29. VipNet. Ключи защиты, мастер ключи, ключи ЭЦП. Особенности ключевой структуры ViPNet. Этапы формирования ключевой информации.
30. Использование аппаратных ключей защиты eToken и HASP для защиты ПО и информации пользователей.
31. Методы, способы и средства защиты информации. Удостоверяющие центры ViPNet
32. Виды угроз безопасности в ТКС. Криптографические системы и их использование в VipNet.
33. ViPNet – сервер открытого Интернета. Транспортный модуль MFTP. Деловая почта. VPN как средство информационной защиты. Центры сертификации – назначение, техническая реализация.
34. Понятие – информационная безопасность. Информационная безопасность в сфере компьютерных сетевых технологий. Протокол https, криптопротоколы SSL, TLS.
35. Защита почтовых систем. Защита серверов и рабочих станций. Защита программного обеспечения – общие подходы и принципы. Электронные цифровые сертификаты. Принцип работы. Формальное описание. Структура сертификата. Российские стандарты.
36. Защита программного обеспечения с помощью аппаратных ключей серии Guardant
37. Семейство электронных ключей Guardant для защиты программного обеспечения от несанкционированного копирования и распространения.
38. Частные сети (VPN): принципы построения, конфигурирование, варианты реализации.
39. Защита программного обеспечения с помощью аппаратных ключей HASP HL, Hasp 4.
40. Электронный ключ (аппаратный ключ). Принципы работы, классификация, примеры использования.
41. Хеш. Хеш-функция. Хеширование. Аутентификация, авторизация, идентификация.
42. Ключи серий ruToken и eToken – сравнительная характеристика, область применения.
43. Технологии аутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера. Рутокен Web.
44. Компьютерные вирусы. Классификация вирусов. Антивирусная защита компьютерной сети. Классификация антивирусов. Основные признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.
45. Обеспечение безопасности web-серверов. Безопасность web-содержимого. Электронные цифровые сертификаты; SSL/TLS; Рутокен Web.

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.