МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный
экономический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки	09.03.03 «Прикладная информатика»
Направленность (профиль) программы	«Управление бизнес-процессами и проектами»
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 11

4. ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТА 13

5. ПЕРЕЧЕНЬ ЗАДАНИЙ ПО ДИСЦИПЛИНЕ 14

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ 16

7. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ 18

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 проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе

1.2. Конечными результатами обучения по дисциплине являются сформированные «знать», «уметь», «владеть», расписанные по отдельным содержательным компонентам компетенций, формирующихся дисциплиной. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы. Планируемые результаты обучения по дисциплине, 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**
ПК-1	Информационная безопасность	Декомпозиция IV Знать: основные методологические аспекты необходимости обследования организаций, выявления информационные потребности пользователей, формирования требований к информационной системе З (IV) (ПК-1) Уметь: проводить всестороннее обследование организаций с целью оценки её текущего состояния в области информационных процессов и систем, выявлять информационные потребности пользователей, формировать требования к информационной системе У (IV) (ПК-1) Владеть: сводами знаний в ИТ-сфере, стандартами, нотациями и инструментальными средствами обследования, описания и моделирования состояния организации в области зрения информационных процессов и систем, выявлять информационные потребности пользователей, формировать требования к информационной системе В(IV)(ПК-1)

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

– различает основные типы информации, хранимые на компьютере;

– использует готовые компьютерные модели, оценивает их соответствие реальному объекту;

– выполняет решение перевода чисел из одной системы счисления в другую;

– определяет необходимый объем памяти для хранения чисел в двоичной системе;

– проводит основные операции над объектами в табличном процессоре (ячейками, столбцами и строками, листами);

– проводит основные операции над объектами в текстовом процессоре.

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
6-ой семестр				
Тема 1. Предпосылки становления предметной области информационной безопасности.	Текущий контроль	Анализ феномена расширения области информационных угроз с развитием информационных технологий. Экономическая и информационная безопасность предприятия.	ПЗ: Решение практических задач по идентификаци и ключевых вопросов ИБ.	Письменная, ПК
Тема 2. Ключевые вопросы информационной безопасности	Текущий контроль	Общие ключевые вопросы комплексной информационной безопасности (ИБ).	ПЗ: Решение практических задач разработке корпора-тивной концепции ИБ.	Письменная, ПК
Тема 3. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	Текущий контроль	Национальная политика и доктрина информационной безопасности. Уровни реализации ИБ и концепция ИБ Российской Федерации. Концепция информационной безопасности Российской Федерации. Концептуальное видение	ПЗ: Решение практических задач по правовым аспектам ИБ.	Письменная, ПК

		проблемы информационной защищенности компании.		
Тема 4. Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	Текущий контроль	Введение понятий информационного права. Базовые элементы информационного правоотношения и основные правоустанавливающие документы. Государственная политика в сфере ИБ. Российское и зарубежное законодательство в области информационной безопасности	ПЗ: Решение практических задач по формировани ю базовых элементов инф. правоотношен ия в организации.	Письменная, ПК
Тема 5. Виды защищаемой информации, Модель угроз и модель информационной безопасности	Текущий контроль	Ключевые вопросы ИБ безопасности современного предприятия. Общая классификация охраняемой информации Концептуальная модель защиты от угроз и алгоритм формирования процесса управления ИБ. Формирование процесса оценки защищенности информационной среды.	ПЗ: Решение практических задач построению модели угроз.	Письменная, ПК
Тема 6. Понятие защищенной информационной системы. Программа информационной безопасности	Текущий контроль	Концептуальные требования защищенности корпоративной ИС. Определение защищенности ИС, необходимое и достаточное условие безопасности ИС. Концепция гарантированности безопасности ИС Понятие и уровни ответственности в информационной сфере.	ПЗ: Решение практических задач по разработке корпоративно й программы создания ИБ.	Письменная, ПК
Тема 7. Организационно-распорядительные документы в сфере информационной безопасности. Общая и частные политики информационной безопасности.	Текущий контроль	Иерархия организационно-нормативных документов и уровень базовых документов в иерархии. Правила разработки и реализации политики ИБ, взаимосвязь и детализация частных политик. Корпоративные стандарты ИБ и организационно-распорядительные документы	ПЗ: Решение практических задач по формировани ю политик ИБ.	Письменная, ПК

Тема 8. Управление информационными рисками	Текущий контроль	Взаимосвязь процессов управления бизнесом и управления экономической и информационной безопасностью в компании. Специфика информационных рисков. Общая схема менеджмента ИТ-рисков, базовые компоненты системы управления рисками.	ПЗ: Решение практических задач по управлению информационными рисками КТ № 1: Презентация	Письменная, ПК
Тема 9. Стандартизация в сфере информационной безопасности	Текущий контроль	Определение стандарта, уровни представления стандартов. Приоритетные направления разработки стандартов в сфере информатизации, роль стандартов информационной безопасности. Содержание этапов стандартизации, объекты стандартизации в открытой информационной системе.	ПЗ: Решение практических задач по использованию стандартов ИБ в деятельности организации.	Письменная, ПК
Тема 10. Математические модели систем и процессов защиты информации	Текущий контроль	Место математических моделей в реализации защиты информации. Математические модели процессов и систем защиты информации (СЗИ). Общие требования к модели СЗИ, этапы построения модели СЗИ результаты практического моделирования. Декомпозиция модели СЗИ, контроль параметров состояния СЗИ (метрики моделей), пример модели процесса защиты	ПЗ: Решение практических задач по построение мат. моделей ИБ.	Письменная, ПК
Тема 11. Сервисы ИБ и защита от инсайдеров	Текущий контроль	Феномен инсайдера в проблеме реализации ИБ, общие характеристики инсайдеров, статистический портрет инсайдера. Механизмы целостности и контроля защищенности данных и сообщений, пример комплексного программного решения, включающего защиту от	ПЗ: Решение практических задач по построение мат. моделей ИБ.	Письменная, ПК

		инсайдеров.		
Тема 12. Криптографические методы защиты информации	Текущий контроль	Криптографические методы защиты информации. Шифрование данных и информации, виды практического шифрования. Требования к криптографическим СЗИ Управление криптографическими ключами. Электронная цифровая подпись, схема системы ЭЦП на базе алгоритма шифрования RSA	ПЗ: Решение практических задач по разработке системы комплексной ИБ. КТ № 2: Презентация	Письменная, ПК
Тема 13. Защита информационной инфраструктуры от атак. Антивирусные средства защиты	Текущий контроль	Взлом защиты информационной инфраструктуры и вирусная опасность. Компьютерные вирусы: классификация, формы организации вирусных атак, виды вредоносного программного обеспечения. Концептуальные положения корпоративной организации защиты от взломов и вирусной опасности, общие требования к антивирусной защите и правила для пользователей.	ПЗ: Решение практических задач по разработке системы комплексной ИБ. КТ № 2: Презентация	Письменная, ПК
Тема 14. Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ	Текущий контроль	Базовая особенность сетевых распределенных информационных структур, общие угрозы в распределенной среде. Четырехуровневая модель защиты распределенной системы Формирование интегральной системы ИБ, схема организации интегральной защиты информационной инфраструктуры и ресурсов, состав средств интегральной защиты. Оценка экономической эффективности интегральной системы ИБ. Развитие методов интегральной защиты.	ПЗ: Решение практических задач по разработке системы комплексной ИБ. КТ № 2: Презентация	Письменная, ПК

7-й семестр				
Тема 15. Идентификация пользователя в информационно-вычислительной системе	Текущий контроль	Методы и инструменты идентификации пользователя в информационно-вычислительной системе	ПЗ: Решение практических задач по отработке навыков использования различных систем доступа в систему и в сеть. КТ № 3: Показ результатов на компьютере	Письменная, ПК
Тема 16. Идентификация пользователя в сети	Текущий контроль	Методы и инструменты идентификации пользователя в информационно-вычислительной сети	ПЗ: Решение практических задач по отработке навыков использования различных систем доступа в систему и в сеть. КТ № 3: Показ результатов на компьютере	Письменная, ПК
Тема 17. Программное приложение KeyLemon	Текущий контроль	Цели и задачи программного приложения KeyLemon Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использования различных систем доступа в систему и в сеть. КТ № 3: Показ результатов на компьютере	Письменная, ПК
Тема 18. Системы шифрования дисковых данных. Технология BitLocker	Текущий контроль	Цели и задачи технологии BitLocker Примеры использования в задачах шифрования дисковых данных	ПЗ: Решение практических задач по отработке навыков использования различных	Письменная, ПК

			программных пакетов.	
Тема 19. Системы шифрования дисковых данных. Технология BitLocker To Go	Текущий контроль	Цели и задачи технологии BitLocker To Go Примеры использования в задачах шифрования дисковых данных	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Тема 20. Шифрование файлов	Текущий контроль	Методы и инструменты шифрования файлов Примеры использования в задачах шифрования файлов	ПЗ: Решение практических задач по отработке навыков использовани я систем шифрования. КТ № 4: Показ результатов на компьютере	Письменная, ПК
Тема 21. Шифрование дисковых данных под Linux	Текущий контроль	Методы и инструменты шифрования дисковых данных под Linux Примеры использования в задачах шифрования дисковых данных	ПЗ: Решение практических задач по отработке навыков использовани я систем шифрования. КТ № 4: Показ результатов на компьютере	Письменная, ПК
Тема 22. Пакет McAfee Endpoint Encryption	Текущий контроль	Цели и задачи пакета McAfee Endpoint Encryption Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Тема 23. Пакет Symantec Drive Encryption	Текущий контроль	Цели и задачи пакета Symantec Drive Encryption Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Тема 24. Пакет Jetico BestCrypt	Текущий контроль	Цели и задачи пакета Jetico BestCrypt	ПЗ: Решение практических	Письменная, ПК

		Функции, экранные формы, настройки и примеры использования	задач по отработке навыков использовани я различных программных пакетов.	
Тема 25. Пакет TrueCrypt	Текущий контроль	Цели и задачи пакета TrueCrypt Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Тема 26. Система Symantec Desktop Email Encryption	Текущий контроль	Цели и задачи системы Symantec Desktop Email Encryption Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Тема 27. Система PGP NetShare	Текущий контроль	Цели и задачи системы PGP NetShare Функции, экранные формы, настройки и примеры использования	ПЗ: Решение практических задач по отработке навыков использовани я различных программных пакетов.	Письменная, ПК
Все темы	Промежуточ-ная аттестация	Обобщенные результаты обучения по дисциплине теоретических знаний и практических навыков	Вопросы	Устная
Итоговый контроль по дисциплине		Вопрос 1. Знать законодательные и нормативно-правовые документы, регулирующие вопросы формирования и использования систем защиты информационных ресурсов. Знать международные и отечественные стандарты в области информационной безопасности Вопрос 2. Уметь использовать законодательные, нормативно-правовые и стандартизирующие	Вопросы к ГИА	

		документы в целях создания и использования системы информационной безопасности и защиты данных в организации Вопрос 3. Владеть: методикой формирования профилей законодательных, нормативно-правовых документов, международных и отечественных стандартов проектах по формированию системы информационной безопасности.		

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	Отсутствие участия в обсуждении, решении,	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе	Высказывание неординарных суждений, активное

	индивидуальных практических задач	неправильное решение		решения, правильное решение с отдельными замечаниями	участие в ходе решения, правильное решение без ошибок
5	Выполнение лабораторной работы	Выполнено менее 54%	Выполнено выше 54% до 69 %	Выполнено от 70% до 84 %	Выполнено выше 85%

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 в 6-ом семестре является зачет, итоговый результат формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<55	Незачет
>=55	Зачет

Формой итогового контроля по дисциплине в 7-ом семестре 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 занятия
Практическая работа	Формирование практических навыков по формированию модели информационной безопасности компании организации с использованием современных подходов реализации систем защиты информации и данных. Построение модели архитектуры бизнеса компании и содержание проектного управления ИБ
	Формирование практических навыков по реализации проекта по разработке системы информационной безопасности с применением современных методов системного и процессного подходов
	Разработка системы организационно-распорядительных документов в рамках системы ИБ: концепция информационной защиты организации, программа разработки ИБ, общая и частные политики реализации ИБ
	Формирование и отработка практических навыков по использованию современных международных стандартов в области защиты информации
	Формирование и отработка практических навыков по использованию различных программных приложений, используемых для формирования эффективной системы комплексной информационной безопасности организации.

5.2. КОНТРОЛЬНЫЕ ТОЧКИ БРС

Контрольная точка № 1. Предпосылки становления и развития предметной области обеспечения информационной безопасности современной организации. Общие принципы формирования и управления информационной безопасностью.

Примерные темы рефератов, эссе и кейсов:

1. Экономическая и информационная безопасность предприятия
2. Правовые вопросы формирования информационной безопасностью предприятия
3. Доктрина РФ в области информационной безопасности
4. Ключевые вопросы организации системы защиты информации современного предприятия
5. Концепция и программа информационной безопасности организации
6. Оценка защищенности корпоративных информационных ресурсов
7. Система организационно-распорядительных документов сфере ИБ. Роль и значение общей и частных политик ИБ

Контрольная точка № 2. Управление рисками ИБ. Вопросы стандартизации в сфере ИБ. Формирование комплексной безопасности современной организации

Примерные темы рефератов, эссе и кейсов:

1. Управление информационными рисками
2. Общие и практические вопросы стандартизации при построении системы ИБ
3. Использование математических моделей в целях организации информационной защиты
4. Современные сервисы обеспечения информационной безопасности и защиты от инсайдеров
5. Содержание криптографических методов защиты корпоративной информации и данных
6. Методы и инструменты защиты информационной инфраструктуры от внешних атак
7. Антивирусные средства защиты информационных ресурсов

8. Организация комплексной защиты информации и данных.

Контрольные точки № 3 и № 4. Применение современных программных пакетов для организации защиты корпоративных данных, информации и знаний

Примерные темы рефератов, эссе и кейсов:

1. Системы идентификации пользователей в информационно-вычислительных системах и сетях
2. Программные приложения для шифрования дисковых данных
3. Шифрование файлов и дисковых данных под Linux
4. Программные пакеты для шифрования и защиты данных McAfee Endpoint Encryption,
Symantec Drive Encryption, Jetico BestCrypt, TrueCrypt, Symantec Desktop Email Encryption, PGP NetShare

5.3. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

ВОПРОСЫ К ЭКЗАМЕНУ:

1. Что является содержанием понятия «экономическая безопасность предприятия?
2. Как можно охарактеризовать понятие «информационная безопасность» и что оно в себя включает (основные составляющие)?
3. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?
4. Какие вопросы информационной безопасности являются ключевыми?
5. Из чего складывается инфраструктура информационной безопасности?
6. Какие существуют виды угроз информационной безопасности и каким образом оцениваются соответствующие риски?
7. На какие виды подразделяется защищаемая информация?
8. На основании каких законов Российской Федерации осуществляется правовое обеспечение и взаимодействие в информационной сфере?
9. Что такое персональные данные? В каком законе Российской Федерации и каким образом отражены аспекты защиты персональных данных?
10. Что составляет базовую суть закона Российской Федерации «Об электронной цифровой подписи»?
11. Как распределяется ответственность в информационной сфере? Во внешней среде предприятия? Во внутренней среде?
12. К каким последствиям могут привести результаты воздействия реализовавшихся угроз на деятельность предприятия?
13. Что такое «Программа информационной безопасности» и сколько уровней она имеет?
14. Что включает в себя модель информационной безопасности?
15. В каких аспектах рассматриваются мероприятия по защите информации?
16. Перечислите основные этапы обеспечения информационной безопасности
17. Для чего необходимо формировать политику информационной безопасности?
18. Из каких основных разделов состоит общая политика информационной безопасности предприятия?
19. Кто разрабатывает политику информационной безопасности предприятия? Какие менеджеры и специалисты входят в рабочую группу?
20. На каком этапе оценки воздействия угрозы возникает понятие информационного риска?
21. Какие методы и инструменты управления рисками можно использовать при формировании информационной защиты?

22. Каким образом оценивается соотношение эффективности и рентабельности систем информационной безопасности?

23. Какие дефекты защиты информации встречаются наиболее часто?

24. В каком случае информационная система считается защищенной?

25. Каким образом архитектура информационной системы может способствовать общей информационной безопасности и почему?

26. В каком стандарте отражены общие вопросы выявления и оценки уязвимости информационных систем?

27. В чем заключается концепция гарантированности безопасности информационных систем?

28. Из каких элементов состоит трёхуровневая модель оценки защищенности информационной системы?

29. Какими путями осуществляется стандартизация подходов к обеспечению информационной безопасности, и какие международные стандарты для этого применяются?

30. Каким образом проводится анализ защищенности ИС?

31. Какие уровни реализуются в технологической модели подсистемы информационной безопасности ИС?

32. Какие угрозы существуют в распределенной (сетевой) среде?

33. Какие средства защиты информации используются в сетевых структурах?

34. С какой целью производится шифрование данных и информации, и на каком уровне работы с информацией это применяется?

35. Чем отличается схема симметричной криптосистемы с закрытым ключом от схемы асимметричной криптосистемы с открытым ключом? Приведите примеры обоих алгоритмов.

36. Что такое хэш-функции? В каких случаях и с какой целью они применяются?

37. Какие стандарты используются в сфере криптографической защиты информации?

38. В каких случаях и с какой целью применяется цифровая подпись?

39. Какие Internet-службы и протоколы могут иметь уязвимости?

41. В каких случаях используются межсетевые экраны?

42. Чем отличается фильтрующий маршрутизатор от шлюза сеансового уровня?

43. Что такое VPN, и для каких целей используются эти технологии?

44. Какие типы вирусов выделены в настоящее время?

45. Какие существуют общие правила для пользователей для обеспечения антивирусной безопасности?

46. Каким общим требованиям должен удовлетворять качественный антивирусный программный продукт?

47. Что такое биометрическая защита, и для каких целей она применяется?

48. В чем заключается интегральный подход к организации информационной защиты? Какие составляющие включает интегральная безопасность информационных систем?

49. Что такое токен и с какой целью используются токены? В каких случаях применяются цифровые маркеры?

50. С какой целью применяется инфраструктура открытых ключей?

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ

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

Комплект оценочных средств хранится на кафедре, подлежит обновлению по мере необходимости. Для промежуточной аттестации в виде экзамена каждое ОС 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).

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 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 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.
	Слабовидящие. Способ восприятия информации: зрительно-осязательно-слуховой	
С нарушениями слуха	Глухие. Способ восприятия информации: зрительно-осязательный	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.
	Слабослышащие. Способ восприятия информации: Зрительно-осязательно-	

	слуховой	
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 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.