Приложение к ОПОП
«Безопасность и этика искусственного интеллекта»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

РАБОЧАЯ ПРОГРАММА

дисциплины

«АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2021

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.т.н. Краснов С.А.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ 02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИБ
Общая трудоемкость (ЗЕТ)	4
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	17
Практические занятия (академ. часов)	34
Все контактные часы (академ. часов)	51
Самостоятельная работа, включая часы на контроль (академ. часов)	93
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

Дисциплина формирует знания, умения и навыки необходимые для защиты информации в компьютерных системах с применением современных аппаратно-программных средств защиты информации. В рамках дисциплины изучаются следующие основные темы: Основные понятия программно-аппаратной защиты информации, принципы её построения. Задачи программно-аппаратной защиты информации. Нормативные документы, посвященные вопросам применения программно-аппаратных средств защиты информации. Методы и средства защиты информации от НСД. Идентификация и аутентификация пользователей. Разграничение доступа. Доверенная загрузка. Изолированная программная среда. Программно-аппаратные механизмы защиты ОС специального назначения. Механизмы защиты сертифицированных антивирусных средств. Практические часть курса, в составе практических работ, нацелена на закрепление материала и получение навыков по настройке аппаратно-программных средств защиты информации по определенным правилам, установленным нормативными или нормативно-методическими документами.

SUBJECT SUMMARY

«HARDWARE AND SOFTWARE FOR INFORMATION PROTECTION IN COMPUTER SYSTEMS»

The discipline forms the knowledge, skills and abilities necessary to protect information in computer systems using modern hardware and software for information protection.

Within the framework of the discipline, the following main topics are studied: Basic concepts of software and hardware protection of information, the principles of its con-struction. Tasks of software and hardware information protection. Regulatory

documents on the use of software and hardware for information protection. Methods and means of protecting information from tampering. User identification and authentication. Access control. Trusted download. Isolated software environment. Hardware and software protection mechanisms for special-purpose OS. Protection mechanisms of certified antivirus products.

The practical part of the course, as part of practical work, is aimed at consolidating the material and acquiring skills in setting up hardware and software for information protection according to certain rules established by regulatory or regulatory and methodological documents.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Цель освоения дисциплины направлена на изучение моделей и методов информационной безопасности требуемых при проектировании и разработке различных систем на основе технологий искусственного интеллекта и приобретение навыков для решения профессиональных задач в различных сферах деятельности

2. Основными задачами изучения дисциплины являются:
– формирование комплексных знаний об основных тенденциях развития технологий искусственного интеллекта, связанных с обеспечением информационной безопасности;
– формирование практических навыков применения средств защиты информации, использующих технологии систем искусственного интеллекта, при решении профессиональных задач.

3. В результате освоения дисциплины обучающийся будет знать основные методы и технологии в области защиты информации, использующие технологии искусственного интеллекта, применяемые в аппаратно-программных средствах защиты информации, а также направления и перспективы их развития.

4. Результатом освоения дисциплины является приобретения умений по настройке механизмов защиты информации, в том числе основанных на технологиях искусственного интеллекта в аппаратно-программных средствах защиты информации с учетом требований информационной безопасности в различных предметных областях

5. Результатом освоения дисциплины является приобретение практических навыков учета всесторонних негативных воздействий злоумышленника на компьютерные системы при разработке, модернизации и администрирование ап-

паратно-программных средств защиты информации, в том числе основанных на технологиях систем искусственного интеллекта, с учетом требований информационной безопасности в различных предметных областях.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Машинное обучение»
2. «Криптография и криптографические протоколы»
3. «Машинное обучение в приложениях биометрии»
4. «Представление знаний в системах искусственного интеллекта»
5. «Управление разработкой промышленного программного обеспечения»

и обеспечивает подготовку выпускной квалификационной работы.

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ПК-31	Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта
ПК-31.2	*Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области*
ПК-32	Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем, основанных на знаниях, по обеспечению требуемых критериев эффективности и качества функционирования
ПК-32.2	*Проводит экспериментальную проверку работоспособности систем, основанных на знаниях*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	СР, ач
1	Ведение	2		1
2	Тема 1 Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.	4	3	10
3	Тема 2 Методы и средства защиты информации от НСД.	5	19	41
4	Тема 3. Методы и средства и антивирусной защиты.	4	12	35
5	Заключение	2		6
	Итого, ач	17	34	93
	Из них ач на контроль	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4		

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Ведение	Предмет, цель и задачи дисциплины. Порядок изучения дисциплины. Рекомендуемая литература. Роль аппаратно-программных методов защиты информации при построении комплексной системы информационной безопасности. Основные понятия и определения. Основные понятия и положения защиты информации в АС. Этапы развития АС. Классификация задач, решаемых с использованием АС. Модели данных, систем и процессов защиты информации в АС. Требования к моделям защиты информации в АС.

№ п/п	Наименование темы дисциплины	Содержание
2	Тема 1 Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.	Руководящие документы средства вычислительной техники, системы обнаружения вторжений, межсетевые экраны, антивирусы, средства защиты от несанкционированного доступа, средства гарантированного уничтожения информации. Сертификация средств защиты информационных систем.Критерии и классы защищенности средств вычислительной техники, и АС СН. Требования к системам защиты информации. Особенности современных АС как объектов информационного воздействия, критерии оценки их защищенности. Уязвимости информационно технологических ресурсов АС. Основные угрозы безопасности информации АС и их классификация. Понятие модели нарушителя в автоматизированной системе.
3	Тема 2 Методы и средства защиты информации от НСД.	Рекомендации по выбору средств защиты. Технологи ческие процедуры парольной политики, использования других средств идентификации и аутентификации, криптографических средств. Основные методы защиты информации. Понятие метода защиты информации. Характеристика основных методов ЗИ. Аппаратно-программные средства ЗИ. Методы эталонных характеристик. Понятие и классификация средств ЗИ. Вспомогатель ные программно-аппаратные средства. Архитектура и компоненты СЗИ от НСД SecretNet + ПАК ”Соболь” и Dallas Lock + смарт-карты. Механизмы защиты ОС специального назначения.
4	Тема 3. Методы и средства и антивирусной защиты.	Общие сведения о компьютерных вирусах. Организация антивирусной защиты. Характеристика сертифицированных антивирусных средств. Противодействие компьютерным вирусам. Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты КС в ходе её эксплуатации. Установка и настройка средств антивирусной защиты. Опытная эксплуатация. Анализ уязвимостей
5	Заключение	Краткий обзор дисциплины. Проблемы обеспечения ИБ современных информационных систем. Перспективы и тенденции развития.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Обоснование и выбор сертифицированных средств защиты информации	4
2. Установка и настройка системы защиты информации от НСД «DALLAS LOCK+ смарт-карты»	6
3. Установка и настройка системы защиты информации от НСД «SECRET NET+ ПАК ”Соболь”»	8
4. Установка и настройка системы защиты информации от НСД В ОС СН «ASTRA LINUX»	8
5. Установка и настройка средств защиты информации в локальных вычислительных сетях при межсетевом взаимодействии.	4
6. Установка и настройка средства антивирусной защиты «KASPERSKY ENDPOINT SECURITY ДЛЯ «WINDOWS»	4
Итого	34

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	15
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	5
Самостоятельное изучение разделов дисциплины	10
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	18
Подготовка к контрольным работам, коллоквиумам	10

Текущая СРС	Примерная трудоемкость, ач
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	93

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Прохорова, Ольга Витольдовна. Информационная безопасность и защита информации [Текст] : учеб. / О. В. Прохорова, 2020. -121 с.	39
2	Воробьев, Евгений Германович. Планирование защиты и контроля безопасности информации в компании в терминах, таблицах и рисунках [Текст] : учеб. пособие / Е. Г. Воробьев, А. К. Племянников, В. Н. Сабынин, 2017. -36 с.	30
3	Воробьев, Евгений Германович. Планирование защиты и контроля безопасности информации в компании в терминах, таблицах и рисунках [Текст] : учеб. пособие / Е. Г. Воробьев, А. К. Племянников, В. Н. Сабынин, 2017. -36 с.	30
4	Краснов, Сергей Александрович. Настройка средств защиты компьютерной информации [Текст] : учеб.-метод. пособие / С. А. Краснов, А. К. Племянников, Д. А. Решетняк, 2020. -71 с.	30
Дополнительная литература		
1	Щеглов, Андрей Юрьевич. Защита информации: основы теории [Текст] : учеб. для бакалавриата и магистратуры для вузов по инженер.-техн. направлениям / А. Ю. Щеглов, К. А. Щеглов, 2019. -308, [1] с.	32

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Федеральная служба по техническому и экспортному контролю (ФСТЭК России) http://fstec.ru/
2	ФСБ России http://fsb.ru/
3	Правительство России http://government.ru/
4	Портал уполномоченного органа по защите прав субъектов персональных данных https://pd.rkn.gov.ru/
5	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций http://rkn.gov.ru/
6	Росстандарт http://www.gost.ru/
7	Единая база ГОСТОВ РФ http://gostexpert.ru/
8	Информационно-правой портал ”Гарант” http://garant.ru/

№ п/п	Электронный адрес
9	Информационно-правой портал ”Консультант” http://consultant.ru/
10	ИСПДН. Защита персональных данных http://www.ispdn.ru/
11	Сайт -Искусство управления информационной безопасностью http://iso27000.ru/
12	Материалы по безопасности от SecurityLab. http://www.securitylab.ru/
13	Ассоциация пользователей стандартов по информационной безопасности АБИСС http://abiss.ru/standards/document_library/
14	Сайт компании ”Код Безопасности” https://www.securitycode.ru/
15	Сайт компании ”Конфидент” https://dallaslock.ru/
16	Сайт компании «Лаборатория Касперского» https://www.kaspersky.ru/
17	Сайт компании ГК Astra Linux https://astralinux.ru/
18	Сайт компании «Доктор Веб» https://www.drweb.ru/
19	Макаренко С. И., Ковальский А. А., Краснов С. А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. – СПб.: Наукоемкие технологии, 2020.: https://www.elibrary.ru/download/elibrary_43141880_41377999.pdf
20	Нечай А.А., Краснов С.А., Свинарчук А.А. Аналитическая модель обеспечения информационной безопасности образовательных организаций системы высшего и среднего образования. Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2020. № 4.: https://www.elibrary.ru/download/elibrary_44408038_85728433.pdf
21	Пилькевич С.В., Гнидко К.О., Сабиров Т.Р., Лохвицкий В.А., Краснов С.А., Дудкин А.С., Иванов О.С. Программное средство выявления ключевых признаков негативного интернет-контента в мультимедийных объектах на основе метода латентно-семантического анализа с динамическим определением ранговых значений. Свидетельство о регистрации программы для ЭВМ RU 2019616036, 16.05.2019. Заявка № 2019614820 от 24.04.2019.: https://www.elibrary.ru/download/elibrary_39315208_18189980.PDF
22	Борисов А.А., Краснов С.А., Нечай А.А. Технология блокчейн и проблемы её применения в различных информационных системах. Вестник Российского нового университета. Се рия: Сложные системы: модели, анализ и управление. 2018. № 2.: https://www.elibrary.ru/download/elibrary_35121901_51404397.pdf

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=7514

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Аппаратно-программные средства защиты информации в компьютерных системах» формой промежуточной аттестации является экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	оценка выставляется студенту, продемонстрировавшему существенные пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий.
Удовлетворительно	оценка выставляется студенту, продемонстрировавшему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, обладающему необходимыми знаниями, но допустившему неточности в ответах на аттестационном испытании и при выполнении учебных заданий.
Хорошо	оценка выставляется студенту, продемонстрировавшему полное знание учебного материала, успешно выполнившему предусмотренные программой задачи, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.
Отлично	оценка выставляется студенту, продемонстрировавшему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоившему основную литературу и ознакомившемуся с дополнительной литературой, рекомендованной рабочей программой дисциплины, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебного материала.

Особенности допуска

К сдаче экзамена допускаются обучающиеся, выполнившие все требования учебной программы: прошедшие контрольные точки (4 коллоквиума по темам изучаемой дисциплины), выполнившие и защитившие все практические работы.

Экзамен проводится в устной форме по билетам, содержащим два теоретических вопроса и практическую задачу. Совокупность оценок, полученных студентом в результате контрольных мероприятий учитывается преподавателем при проведении промежуточной аттестации в форме экзамена. При этом оценка по результатам текущего контроля составляет 60% от общей итоговой оценки, экзаменационная -40%.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Примерные вопросы к экзамену

№ п/п	Описание
1	Перечислите классы защищенности СВТ от НСД к информации и кратко охарактеризуйте их.
2	Перечислите и охарактеризуйте методы и способы защиты программ от исследования.
3	Произвести настройку системы контроля целостности в СЗИ от НСД Secret Net 7.6 для папки указанной преподавателем.
4	Перечислите классы защищенности АС и кратко охарактеризуйте их. Для каких классов АС необходима криптографическая подсистема?
5	Перечислите и охарактеризуйте методы, способы и алгоритмы защиты программы от модификации.
6	Перечислите и охарактеризуйте методы, способы и алгоритмы защиты программы от копирования.
7	Дайте определение угрозы ИБ. Чем отличается нарушитель ИБ от злоумышленника? Каковы источники угроз безопасности АС и информации? Приведите примеры.
8	Расскажите об общих требованиях по обеспечению ИБ средствами антивирусной защиты.
9	Дайте определение понятия «уязвимость». Перечислите признаки классификации уязвимостей. Приведите примеры классификации уязвимостей.
10	Перечислите основные методы зашиты (защитные механизмы) компьютерных систем и кратко охарактеризуйте их.

11	Перечислите основные меры по защите информации в КС и кратко охарактеризуйте их. Приведите достоинства и недостатки различных видов мер защиты.
12	Перечислите основные угрозы безопасности информации, возникающие при взаимодействии с сетями общего пользования. Перечислите функции СЗИ НСД на абонентском пункте при работе в сети.
13	Перечислите основные виды вредоносных программ. Перечислите признаки классификации программных вирусов и сетевых червей и приведите примеры такой классификации.
14	Перечислите стадии создания системы защиты информации и кратко охарактеризуйте их.
15	Перечислите классы защищенности МЭ и дайте их краткую характеристику.
16	Перечислите и кратко охарактеризуйте скрытые угрозы и атаки
17	Перечислите меры по обеспечению информационно-компьютерной безопасности
18	Перечислите и охарактеризуйте уровни защиты компьютерных ресурсов
19	Охарактеризуйте законодательные меры по обеспечению информационной безопасности. Назовите важнейшие законодательные и нормативные акты Российской Федерации в области ИБ.
20	Опишите общие требования государственных стандартов. Требования руководящих документов ФСТЭК России
21	Дайте классификацию программного обеспечения по уровню контроля на отсутствие недекларированных возможностей
22	Аутентификация при доступе к компьютерным ресурсам. Концепция контроля доступа в компьютерную систему и факторы аутентификации
23	Особенности аутентификации в ОС Linux и Windows
24	Особенности применения аппаратных средств аутентификации. Персональные идентификаторы iButton. Смарт-карты РИК. Электронные ключи Рутокен.
25	Перечислите и охарактеризуйте модели управления доступом
26	Охарактеризуйте подсистему контроля целостности и подлинности программного обеспечения. Раскройте принципы его построения и функционирования.
27	Охарактеризуйте подсистему замкнутой программной среды. Раскройте принципы его построения и функционирования.
28	Раскройте принципы функционирования АПМДЗ «Соболь». Идентификация и аутентификация с помощью АПМДЗ «Соболь».
29	Раскройте принципы функционирования АПМДЗ «Соболь». Блокировка загрузки ОС со съемных носителей
30	Раскройте принципы функционирования АПМДЗ «Соболь». Контроль целостности средствами АПМДЗ «Соболь»
31	Опишите особенности управления доступом в ОС Windows и Linux
32	Классификация компьютерных вирусов и программных закладок
33	Построение системы защиты от компьютерных вирусов и программных закладок. Требования к средствам антивирусной защиты (САВЗ)

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ

БИЛЕТ № 1

Дисциплина **Аппаратно-программные средства защиты информации в компьютерных системах**

1. Классификация средств вычислительной техники по уровню защищенности от НСД. Классификация защищенности АС от НСД к информации.

2. Защита программ от исследования. Использование контрольного суммирования для защиты программы от модификации.

3. Произвести настройку системы контроля целостности в СЗИ от НСД Secret Net 7.6 для папки указанной преподавателем.

УТВЕРЖДАЮ

Заведующий кафедрой

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
3	Тема 1 Основные понятия и задачи программно-аппаратной защиты информации, принципы её построения.	
4		Коллоквиум
7	Тема 2 Методы и средства защиты информации от НСД.	
8		Коллоквиум
11	Тема 2 Методы и средства защиты информации от НСД.	
12		Коллоквиум
14	Тема 3. Методы и средства и антивирусной защиты.	
15		Коллоквиум

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий).

на практических занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), сдача 4 коллоквиумов по тематике дисциплины (проверка знаний и умений по каждой теме) по результатам которого студент получает допуск на экзамен. На коллоквиумах проводится защиты работ, которые проводились на практических занятиях.

В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, компьютер или ноутбук, проектор, экран, маркерная доска.	Windows XP и выше; 2) Microsoft Office 2007 и выше, СДО ”Moodle”
Практические занятия	Аудитория	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; Astra Linux SE 1.6 и выше. 2) Microsoft Office 2007 и выше; 3) SecretNet и ПАК ”Соболь”, Dallas lock + смарт-карты, KASPERSKY ENDPOINT SECURITY для «WINDOWS».
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; Astra Linux SE 1.6 и выше. 2) Microsoft Office 2007 и выше, СДО ”Moodle”; 3) SecretNet и ПАК ”Соболь”, Dallas lock + смарт-карты, KASPERSKY ENDPOINT SECURITY для «WINDOWS».

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА