

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.ДВ.04.01
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности критической информационной инфраструктуры
(наименование дисциплины)

по направлению подготовки

09.03.03 Прикладная информатика

направленность (профиль)

Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 53Е

Распределение часов дисциплины по семестрам

Семестр	8	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	12	12
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	60,25	60,25
Самостоятельная работа	119.75	119.75
Контроль	-	-
Итого	180	180

Рабочую программу составил(и):

Доцент ИИиЭБ, к.э.н., доцент, Фрезе Т.Ю.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2030

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от 01.09.2025).

1. Цель освоения дисциплины

Цель освоения дисциплины является изучение основных понятий, методологии и практических приемов обеспечения безопасности объектов критической информационной инфраструктуры.

Задачи изучения дисциплины:

- 1) изучение основных понятий и технологий обеспечения информационной безопасности объектов критической информационной инфраструктуры;
- 2) получение знаний и навыков защиты объектов критической информационной инфраструктуры;
- 3) изучение нормативно-правовых актов, регулирующих вопросы создания, эксплуатации и защиты объектов критической информационной инфраструктуры;
- 4) приобретение обучаемыми необходимого объема знаний в области организации работы по защите объектов критической информационной инфраструктуры;
- 5) формирование у обучаемых целостного представления о внедрении системного подхода к решению задач обеспечения информационной безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: Организационно-правовые нормы обеспечения информационной безопасности.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: Выполнение и защита выпускной квалификационной работы.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управлению БД	ПК-10.10 Использует знания математического и имитационное моделирования систем защиты информации	Знает Математическое и имитационное моделирование систем защиты информации Умеет применять модели процессов в информационном обмене в системах защиты информации, модели процессов сохранения конфиденциальности информации Владеет алгоритмами создания системы комплексной защиты, методологией разработки моделей, инструментарием имитационного моделирования

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.13 Использует знания нормативно-правовых актов и методических документов по защите информации, угрозы безопасности информации КИИ	Знать: - виды конфиденциальной информации, нормативно-правовые акты и методические документы по защите информации, угрозы безопасности информации Уметь: - разрабатывать технические задания на создание системы обеспечения информационной безопасности Владеть: - навыками формирования требований к системе обеспечения информационной безопасности
	ПК-11.14 Умеет определять актуальные угрозы безопасности критической информационной инфраструктуры	Знать: - типы актуальных угроз КИИ
		Уметь: - выявить критические процессы и активы субъекта КИИ - определять актуальные угрозы безопасности информации
		Владеть: - приемами обеспечения безопасности объектов критической информационной инфраструктуры
	ПК-11.15 Владеет навыками формирования требований к системе обеспечения безопасности КИИ	Знать: - требования к обеспечению безопасности КИИ
		Уметь: - организовать и провести категорирование ОКИИ
		Владеть: -навыками проведения классификации информационных систем по требованиям защиты информации

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	<p>Тема 1 Субъекты КИИ: понятие, определение принадлежности</p> <p>1.ФЗ 187 «О безопасности критической информационной инфраструктуры»</p> <p>2.Объекты критической информационной инфраструктуры: основные понятия, термины и определения.</p> <p>3.Права субъектов критической информационной инфраструктуры</p> <p>4.Обязанности субъектов КИИ</p> <p>5.Самоопределение принадлежности к КИИ</p> <p>6. Набор документов для определения является ли организация субъектом КИИ</p> <p>7. Дорожная карта по выполнению требований Федерального закона «О</p>	8	2	-	-	Банк тестовых заданий

		безопасности критической информационной инфраструктуры» 8. Основные понятия, термины и определения в области обеспечения безопасности ЗОКИИ. Система безопасности ЗОКИИ					
Модуль 1	Пр	Практическая работа 1 Самоопределение субъекта по ФЗ 187	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 2 Составление Дорожной карты по выполнению требований законодательства РФ	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 3 Мероприятия по определению оснований для отнесения организации к	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 2 Объекты КИИ: типы и виды 1. Типы объектов КИИ 2. Классификация ОКИИ по значимости 3. Реестр значимых объектов КИИ 4. Классификация ОКИИ по видам систем	8	2	-	-	Банк тестовых заданий

		5. Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ					
Модуль 1	Пр	Практическая работа 4 Оценка объектов КИИ субъекта КИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 3. Категорирование объектов КИИ 1. Правила категорирования объектов критической информационной инфраструктуры 2. Формирование комиссии по категорированию 3. Подготовка перечня объектов КИИ подлежащих категорированию 4. Категорирование (присвоение объекту КИИ категории, либо принятие мотивированного решения об отсутствии необходимости в ее присвоении) 5. Оценка объектов КИИ в соответствии с показателями критериев значимости 6. Подготовка итоговых документов по результатам категорирования	8	2	-	-	Банк тестовых заданий

		7. Сроки категорирования 8. Реестр значимых объектов КИИ. Цель ведения реестра					
Модуль 1	Пр	Практическая работа 5 Проведение инвентаризации объектов КИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 6 Категорирование объектов КИИ	8	4	-	-	Отчет по практической работе
Модуль 1 Тема 3.	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 4 Обеспечение безопасности значимых объектов кии 1. Этапы создания и функционирования СОИБ ЗОКИИ 2. Аудит информационной безопасности ЗОКИИ 3. Моделирование угроз ЗООКИИ 4. Уровень зрелости процессов информационной безопасности по методологии ISF 5. План мероприятий по обеспечению безопасности ЗОКИИ 6. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз	8	2	-	-	Банк тестовых заданий

		безопасности информации и их последствия 7. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей ЗОКИИ, возможных способов реализации (возникновения) угроз безопасности информации и последствий от их реализации					
Модуль 1	Пр	Практическая работа 7 Составление модели угроз ЗОКИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 8 План мероприятий по обеспечению безопасности ЗОКИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 5 Организационные и технические меры по обеспечению безопасности ЗОКИИ 1 Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Требования по обеспечению безопасности ЗОКИИ» 2. Технологии обеспечения безопасности критической	8	2	-	-	Банк тестовых заданий

		информационной инфраструктуры 3. Принципы обеспечения безопасности критической информационной инфраструктуры 4. Состав и содержание организационных и технических мер по обеспечению безопасности ЗОКИИ					
Модуль 1	Пр	Практическая работа 9 Организационные и технические меры по обеспечению безопасности ЗОКИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 6 Взаимодействие с ГОССОПКА. Практические вопросы взаимодействия с регуляторами 1.НПА по порядку взаимодействия с ГОССОПКА 2.Назначение и функции ГОССОПКА, НКЦКИ 3.Структура ГОССОПКА 4. Методы организации взаимодействия 5. Содержание мероприятий 6. Комплект документации	8	2	-	-	Банк тестовых заданий

Модуль 1	Пр	Практическая работа 10 Разработка схемы взаимодействия с ГосСОПКА	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 11 Расчет показателей категории значимости ЗООКИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 12 Методика проектирования и построения схемы защиты объектов КИИ	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	19.75	-	-	Банк тестовых заданий
	ПА	Промежуточная аттестация/ Итоговое тестирование	8	0,25		-	Банк тестовых заданий /Вопросы к зачету
Итого:				180			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
Формы и методы обучения		
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо разобрать их с преподавателем. Подготовка к экзамену необходимо начинать заранее.

Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
8	ПК-11.13, ПК-11.14, ПК-11.15	Отчет по практическим работам №№1-12
		Вопросы к зачету №№1-45
		Банк тестовых заданий №1-15

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическая работа

(наименование оценочного средства)

Практическая работа 1 Самоопределение субъекта по ФЗ 187

Практическая работа 2 Составление Дорожной карты по выполнению требований законодательства РФ

Практическая работа 3 Мероприятия по определению оснований для отнесения организации к

Практическая работа 4 Оценка объектов КИИ субъекта КИИ

Практическая работа 5 Проведение инвентаризации объектов КИИ

Практическая работа 6 Категорирование объектов КИИ

Практическая работа 7 Составление модели угроз ЗОКИИ

Практическая работа 8 План мероприятий по обеспечению безопасности ЗОКИИ

Самостоятельное изучение материала, чтение электронного учебника

Практическая работа 9 Организационные и технические меры по обеспечению безопасности ЗОКИИ

Практическая работа 10 Разработка схемы взаимодействия с ГосСОПКА

Практическая работа 11 Расчет показателей категории значимости ЗООКИИ

Практическая работа 12 Методика проектирования и построения схемы защиты объектов КИИ

Типовой(ые) пример(ы) задания(ий)

Шаблон отчетной формы:

- Акт самоопределения (Заключение о соответствии)
- Организация: [Название]
- Сфера деятельности: (Гос. орган, ОПК, энергетика и пр.)
- Наличие объектов (перечень): (АСУ ТП, информационные системы, сети связи)
- Применимость ФЗ-187: (Применим / Не применим)
- Обоснование: (Со ссылкой на пункты статей закона и ПП РФ №127)
- Дата и подпись

Темы письменных работ

№	Тема
1	Сравнительный анализ подходов к категорированию объектов КИИ в Российской Федерации и странах Европейского союза.

2	Правовые и организационные аспекты взаимодействия субъекта КИИ с НКЦКИ при реагировании на компьютерные инциденты.
3	Оценка рисков и угроз безопасности информации для автоматизированных систем управления технологическими процессами (АСУ ТП) на примере гипотетического объекта энергетики.
4	Импортозамещение программного обеспечения как фактор обеспечения технологической независимости и безопасности КИИ.
5	Методы и средства обнаружения компьютерных атак в промышленных сетях передачи данных.

Краткое описание и регламент выполнения

1. Изучить ст. 2 ФЗ-187 (сфера действия закона).
2. Проанализировать учредительные документы и виды деятельности выданного варианта организации.
3. Проверить наличие у организации прав собственности или иных законных оснований на информационные системы, работающие в критических сферах.
4. Сделать письменное заключение.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.

- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.4 Типовой пример тестового задания

Какой основной критерий лежит в основе присвоения объекту КИИ одной из категорий значимости (первой, второй или третьей) в соответствии с законодательством РФ?

Варианты ответа:

- А. Количество работающих на объекте сотрудников.
- В. Степень тяжести последствий от возможного нарушения функционирования объекта (социальный, политический, экономический, экологический ущерб).
- С. Стоимость программно-аппаратных средств, установленных на объекте.
- Д. Принадлежность объекта к государственной или частной форме собственности.

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

№ п/п	Вопросы к зачету
1.	1. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
2.	Принципы обеспечения безопасности критической информационной инфраструктуры
3.	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
4.	Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры
5.	Категорирование объектов критической информационной инфраструктуры
6.	Реестр значимых объектов критической информационной инфраструктуры
7.	Права и обязанности субъектов критической информационной инфраструктуры
8.	Система безопасности значимого объекта критической информационной инфраструктуры
9.	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
10.	Оценка безопасности критической информационной инфраструктуры
11.	Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры
12.	Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов
13.	Регламентация правил и процедур аудита безопасности
14.	Перечень показателей критериев ЗОКИИ и их значения
15.	Оценка в соответствии с перечнем показателей критериев ЗОКИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ
16.	Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности ЗОКИИ
17.	Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ
18.	Правила категорирования объектов критической информационной инфраструктуры
19.	Каковы этапы создания и функционирования СОИБ ЗОКИИ
20.	Технологии обеспечения безопасности критической информационной инфраструктуры
21.	Принципы обеспечения безопасности критической информационной инфраструктуры
22.	Состав плана мероприятий по СИБ ЗООКИИ
23.	Алгоритм категорирования вновь создаваемых ОКИИ
24.	Порядок изменений в Перечне ОКИИ, подлежащих категорированию
25.	Порядок информирования НКЦКИ об компьютерных инцидентах
26.	Схема взаимодействия с ГОССОПКА
27.	Порядок Перевода не значимого ОКИИ в ЗОКИИ
28.	Порядок исключения ИС/АСУ/ИТКС из объектов КИИ
29.	Порядок реагирования на компьютерные инциденты с ЗОКИИ
30.	Методы организации взаимодействия с ГОССОПКА
31.	Перечень информации, передаваемой в ГосСОПКА

32.	Что делать с объектами КИИ не имеющими категорию значимости: как их учитывать, как это фиксировать, оформлять и т.п.?
33	Порядок обработки замечаний от ФСТЭК (после отправки Перечня объектов КИИ и после отправки сведений об объектах КИИ)
34	С кем нужно согласовывать Перечень объектов КИИ, подлежащих категорированию?
35	Алгоритм перевода ЗОКИИ в незначимые ОКИИ
36	Требования к специалисту безопасности ЗОКИИ
37	Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ
38	Виды контроля (мониторинга) за обеспечением уровня безопасности значимого объекта КИИ и его системы безопасности
39	Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ
40	Порядок документирования процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ
41	Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ
42	Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ
43	Требования к силам обеспечения безопасности значимых объектов КИИ
44	Структура системы безопасности ЗОКИИ
45	Этапы жизненного цикла системы безопасности ЗОКИИ

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Зачет	«зачтено»	практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет теоретическим материалом, отвечает на дополнительные вопросы
		«не зачтено»	практические работы не выполнены или имеют существенные замечания; обучающийся не владеет теоретическим материалом, не отвечает на дополнительные вопросы или отвечает с грубыми ошибками

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Прокопенко, Е. В.	Категорирование объектов критической информационной инфраструктуры : учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2025. — 112 с. — ISBN 978-5-00137-535-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/516391	учебное пособие	2025	Лань : электронно-библиотечная система
2	Макаренко, С. И.	Аудит безопасности критической информационной инфраструктуры : учебное пособие / С. И. Макаренко. — Санкт-Петербург : Наукоемкие технологии, 2023. — 124 с. — ISBN 978-5-907618-78-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/157432.html	учебное пособие	2023	Цифровой образовательный ресурс IPR SMART

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Конев, А. А.	Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры : учебно-методическое пособие / А. А. Конев, А. Ю. Якимук. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2022. — 174 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/152786.html	учебно-методическое пособие	2022	Цифровой образовательный ресурс IPR SMART

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Консультант+	Договор №1522 от 25.12.2015, срок действия - бессрочно
2	Windows: WinPro 10 RUS Upgrd OLP NL Acdmc	договор № 757 от 04.07.2018, срок действия – бессрочно; контракт № 1653 от 14.12.2018, срок действия – бессрочно
3	Office Standard: ⁴ Office Stdandard 2013 Russian OLP NL AcademicEdition	договор № 690 от 19.05.2015, срок действия – бессрочно

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парта двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся Г-401	Стол, стулья, компьютеры
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа.	Стол, стулья, стол преподавательский, стул

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-402	преподавательский, доска аудиторная (меловая), кафедра напольная
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-413	Стол ученические двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая) , кафедра напольная
5	Лаборатория кибербезопасности. Лаборатория «Автоматизированные системы в защищенном исполнении». Лаборатория «Программно-аппаратные средства защиты информации». Лаборатория «Безопасность вычислительных сетей» Лаборатория «Техническая защита информации». Лаборатория «Сети и системы передачи информации». Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования. Аудитория для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Э-101в	Стол компьютерные, стол преподавательский, стулья, шкаф металлический, телевизор на передвижной тумбе, стойка телекоммуникационная, коммутатор оптический Qtech QSW-6910-26F, коммутатор Qtech QSW-4610-28T-AC, система хранения данных Русский щит Alpha DF5045, сервер Русский щит Gamma SX6302, ноутбук Digma Pro Sprint M DN15P3-8CXW02, осциллограф АКИП-4115/1А, анализатор низкочастотных сигналов СКМ-21, генератор сигналов АКИП-3407/1А, антенна дипольная активная Е-3000А1, антенна рамочная Н-30А1, акустический излучатель АС-1 Лайт Арт.001, рефлектометр ТОПА3-7317-ARX, измерительный пробник напряжения ШИП, анализатор спектра АКИП-4211/1, межсетевой экран ССПТ-2

