

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

Б1.В.ДВ.04.02  
(индекс дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Моделирование процессов и средств защиты информации

---

(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	-	-
<b>Итого</b>	<b>180</b>	<b>180</b>

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

Дисциплина «Моделирование процессов и систем защиты информации» относится к группе дисциплин вариативной части образовательной программы. Дисциплина изучается на 3 курсе в 6 семестре.

Целью освоения дисциплины является теоретическая и практическая подготовка студентов по применению методов моделирования и проектирования систем защиты информации.

В процессе освоения дисциплины студент должен научиться выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ.

### 2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: Международные и российские нормативные акты, и стандарты по информационной безопасности, Основы управления информационной безопасностью

Полученные знания используются при изучении следующих дисциплин: Техническая защита информации, Программно-аппаратные средства защиты информации

### 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
		Знает:

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	ПК-10.11 Умеет применять модели процессов в информационном обмене в системах защиты информации	Математическое и имитационное моделирование систем защиты информации
		Умеет: - разрабатывать модели управления рисками информационной безопасности
		Владеет: - навыками построения имитационной модели
	ПК-10.12 Владеет алгоритмами создания системы комплексной защиты, методологией разработки моделей	Знает: - алгоритм создания системы комплексной защиты, методологию разработки моделей
		Умеет: - разрабатывать ролевую матрицу доступа
		Владеет: - инструментарием имитационного моделирования
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

#### 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	Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации. Понятие модели, моделирования, адекватности модели. Цели и задачи моделирования. Процесс моделирования. Типы классификации моделей. Материальные (физические) и идеальные модели. Когнитивные, содержательные, концептуальные, формальные модели. Компьютерные модели. Методы моделирования случайных величин. Задачи имитационного моделирования. Области применения моделей. Этапы построения моделей. Преимущества и недостатки имитационного	8	2	-	-	Банк тестовых заданий

		моделирования. Применение линейных регрессионных моделей эксперимента с помощью компьютерного моделирования.					
Модуль 1	Пр	Практическая работа 1 Моделирование реальных ситуаций, которые могут быть исследованы с помощью дискретно-событийных моделей	8	4			Отчет по практическому занятию №1
Модуль 1	Пр	Практическая работа 2 Создание ЕРС-моделей. Построение моделей.	8	4			Отчет по практическому занятию №2
Модуль 1 Тема 1 Основные понятия теории моделирования. Математическое и имитационное моделирование систем защиты информации	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 2 Алгоритм создания системы комплексной защиты. Методология разработки моделей. Алгоритм создания системы комплексной защиты. Методология разработки моделей. Функции моделирования информационного обмена. Способ перехода от	8	2	-	-	Банк тестовых заданий

		математической модели процесса к цифровой модели: нормировка параметров модели. Модель защиты информации					
Модуль 1	Пр	Практическая работа 3 Разработка модели системы защиты информации	8	4			Отчет по практическому занятию №3
Модуль 1 .	Пр	Практическая работа 4 Разработка модели архитектуры информационной системы	8	4			Отчет по практическому занятию №4
Модуль 1	Пр	Практическая работа 5 Идентификация и оценка рисков	8	4			Отчет по практическому занятию №5
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 3. Модели процессов в информационном обмене в системах защиты информации. Моделирование процессов защиты информации. Разработка модели управления рисками информационной безопасности. Модель процессов контроля информации. Модель процессов воздействия компьютерных вирусов. Модель действий инсайдера.	8	2	-	-	Банк тестовых заданий

Модуль 1	Пр	Практическая работа 6 Обоснование рисковых решений методом «дерева решений»	8	4			Отчет по практическому занятию №6
Модуль 1	Пр	Практическая работа 7 Разработка модели адаптивной системы информационной безопасности, действий инсайдера	8	4			Отчет по практическому занятию №7
	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 4 Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Модель процессов сохранения конфиденциальности информации. Модель процессов сохранения целостности информации. Модель процессов сохранения доступности информации. Модель процессов сохранения неотказуемости. Модель синтеза рационального проекта системы защиты информации.	8	2	-	-	Банк тестовых заданий



Модуль 1	Пр	Практическая работа 8 Разработка модели злоумышленника	8	4			Отчет по практическому занятию №8
Модуль 1	Пр	Практическая работа 9 Анализ рисков информационной безопасности на основе модели угроз и уязвимостей	8	4			Отчет по практическому занятию №9
Модуль 1	Пр	Практическая работа 10 Моделирование инженерно- технической системы защиты информации по исходным данным для объекта информатизации	8	4			Отчет по практическому занятию №10
Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 5 Инструментарии имитационного моделирования  Система моделирования GPSS. Система имитационного моделирования Arena. Методика построения моделей с помощью системы Arena. Создание VACD- модели.	8	2	-	-	Банк тестовых заданий
Модуль 1	Пр	Практическая работа 11 Разработка моделей в продукте Arena 7.0 по составленным ранее EPC- диаграммам	8	4			Отчет по практическому занятию №11

Модуль 1	Ср	Самостоятельное изучение материала, чтение электронного учебника	8	20	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 6 Модели безопасности компьютерных систем Модели безопасности на основе дискретной политики. Модели на основе матрицы доступа. Модели распространения прав доступа. Модель Харисона-Руззо-Ульмана. Модель типизированной матрицы доступа. Модели безопасности на основе мандатной политики. Модели безопасности на основе тематической политики. Модели безопасности на основе ролевой политики.	8	2			
Модуль 1 Тема 6 Модели безопасности компьютерных систем	Пр	Практическая работа 12 Разработка ролевой матрицы доступа	8	4			Отчет по практическому занятию №12
Модуль 1 Тема 6 Модели безопасности компьютерных систем	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
<b>Итого:</b>				<b>180</b>			

## 5. Образовательные технологии

Технология	Формы обучения	Методы обучения
<b>Технология традиционного обучения</b> – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
<b>Технология модульного обучения</b> – 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.
<b>Информационные технологии</b> – 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		
<b>Дистанционное обучение</b>	<b>Сетевая технология</b> – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. <b>CD-технология</b> – 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-10, ПК-11	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 Моделирование реальных ситуаций, которые могут быть исследованы с помощью дискретно-событийных моделей

Практическая работа 2 Создание ЕРС-моделей.

Построение моделей.

Практическая работа 3 Разработка модели системы защиты информации

Практическая работа 4 Разработка модели архитектуры информационной системы

Практическая работа 5 Идентификация и оценка рисков

Практическая работа 6 Обоснование рискованных решений методом «дерева решений»

Практическая работа 7 Разработка модели адаптивной системы информационной безопасности, действий инсайдера

Практическая работа 8 Разработка модели злоумышленника

Практическая работа 9 Анализ рисков информационной безопасности на основе модели угроз и уязвимостей

Практическая работа 10 Моделирование инженерно-технической системы защиты информации по исходным данным для объекта информатизации

Практическая работа 11 Разработка моделей в продукте Arena 7.0 по составленным ранее ЕРС-диаграммам

Практическая работа 12 Разработка ролевой матрицы доступа

#### Типовой(ые) пример(ы) задания(ий)

Таблица 1 - Анализ ситуации.

Ситуация	Сущности	Состояния	Дискретные события (вход/выход)

Вывод: почему ситуация является дискретно-событийной, а не непрерывной.

#### Темы письменных работ

№	Тема
1	Моделирование мандатного управления доступом: модель Белла — Лападулы (BLP).
2	Сравнительное моделирование дискреционных моделей: матрица доступа Харрисона — Руццо — Ульмана (HRU) и граф доступа Такешы — Гиллоя (TG).
3	Моделирование угроз информационной безопасности на основе сетей Петри.
4	Имитационное моделирование политики ролевого доступа (RBAC) с учетом разделения обязанностей (SoD).
5	Математическое моделирование распространения вредоносного ПО (модель SIR в контексте кибербезопасности).

#### **Краткое описание и регламент выполнения**

1. Выбрать две реальные ситуации из списка: обработка входящих заявок в техподдержку, работа очереди печати, прохождение контроля доступа на КПП, инцидент ИБ (например, распространение вируса по сети).
2. Выделить и записать:
3. Сущности (субъекты, объекты, ресурсы);
4. Состояния системы;
5. Дискретные события (начало, завершение, отказ, блокировка);
6. Очереди событий.
7. Построить временную диаграмму последовательности событий для одного сценария.

#### **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**

В модели мандатного доступа Белла — Лападулы (BLP) для субъекта с уровнем секретности «Секретно» (Secret, уровень 3) и объекта с уровнем «Конфиденциально» (Confidential, уровень 2) в иерархии решетки (4 уровня: 0-Несекретно, 1-Конфиденциально, 2-Секретно, 3-Сов. секретно) в состоянии системы, удовлетворяющем свойствам *ss* и \*-свойству, какая операция разрешена?

Варианты ответов:

1. Только запись (Write) субъекта в объект.
2. Только чтение (Read) субъектом объекта.
3. И чтение, и запись.
4. Ни чтение, ни запись.

#### **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.	Основы теории моделирования
2.	Основные термины и определения. Классификация методов моделирования.
3.	Принципы системного подхода в моделировании
4.	Виды показателей эффективности
5.	Выбор уровня описания системы в модели. Методология разработки моделей. Алгоритм создания системы комплексной защиты
6.	Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации
7.	Методы теории игр в информационной безопасности
8.	Моделирование по событиям. Моделирование параллельных процессов
9.	Вероятностная модель системы контроля доступа к информации
10.	Разработка модели управления рисками информационной безопасности
11.	Разработка модели действий инсайдера
12.	Методы определения важности требований к процессам и системам защиты информации
13.	Разработка моделей защиты информации
14.	Стратегическое планирование имитационного экспериментов
15.	Методы оценки адекватности, устойчивости, чувствительности модели
16.	Модель адаптивной системы информационной безопасности
17.	Выбор уровня описания системы в модели. Этапы моделирования
18.	Модель формирования множества функций защиты информации
19.	Моделирование по событиям. Моделирование параллельных процессов
20.	Модели выбора рационального варианта средства защиты информации на основе экспертной информации
21.	Оценка качества имитационной модели. Методы оценки адекватности
22.	Виды показателей эффективности моделей
23.	Методы определения важности требований, предъявляемых к системе защиты информации
24.	Алгоритм создания системы комплексной защиты
25.	Функции моделирования информационного обмена
26.	Определение динамических диапазонов модулируемых процессов
27.	Модель представления информации с учетом надежности программно-аппаратных средств
28.	Модель процессов контроля информации
29.	Модель процессов воздействия компьютерных вирусов
30.	Разработка модели действий инсайдера
31.	Модель процессов сохранения конфиденциальности информации
32.	Модель процессов сохранения целостности информации
33.	Модель процессов сохранения доступности информации
34.	Модель процессов сохранения неотказуемости
35.	Модель синтеза рационального проекта системы защиты информации
36.	Модель адаптивной системы информационной безопасности
37.	Язык GPSS как средство построения моделей
38.	Приемы создания VACD-модели
39.	Модели безопасности на основе дискретной политики

40.	Как создать ролевую матрицу доступа?
41.	Мероприятия по созданию матрицы доступа
42.	Модели безопасности на основе ролевой политики
43.	Модели распространения прав доступа
44.	Методика построения моделей с помощью системы Arena
45.	Моделирование для имитации атак, принципы, цель, способы реализации

Семестр 8

### 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	С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин	Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. - Новосибирск : Изд-во НГТУ, 2023. - 80 с. - ISBN 978-5-7782-4905-9. - Текст : электронный. - URL: <a href="https://znanium.ru/catalog/product/2246196">https://znanium.ru/catalog/product/2246196</a>	учебное пособие	2023	ЭБС ZNANIUM
2	Краковский, Ю. М.	Методы и средства защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 272 с. — ISBN 978-5-507-52958-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/463013">https://e.lanbook.com/book/463013</a>	учебное пособие для вузов	2025	Лань : электронно-библиотечная система

### 8.2. Дополнительная литература



<b>№ п/п</b>	<b>Авторы, составители</b>	<b>Заглавие (заголовок)</b>	<b>Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)</b>	<b>Год издания</b>	<b>Количество в научной библиотеке / Наименование ЭБС</b>
1	Солонская, О. И.	Средства защиты информации : учебное пособие / О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 89 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/117115.html">https://www.iprbookshop.ru/117115.html</a>	учебное пособие	2021	Цифровой образовательный ресурс IPR SMART

### 8.3. Перечень профессиональных баз данных и информационных справочных систем

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

### 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: <sup>4</sup> 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 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 ученические двухместные, стулья, стол преподавательский, стул

№ п/п	<b>Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)</b>	<b>Перечень основного оборудования</b>
	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

