

## **Б1.Б.24 Теория информационной безопасности и методология защиты информации**

### **рабочая программа дисциплины (модуля)**

Закреплена за кафедрой	<b>Информационные технологии и защита информации</b>		
Учебный план	10.03.01 ИБ-2021.plx 10.03.01 Информационная безопасность		
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)		
<b>Квалификация</b>	<b>Бакалавр</b>		
Форма обучения	<b>очная</b>		
Объем дисциплины (модуля)	<b>6 ЗЕТ</b>		
Часов по учебному плану	216	Часов контактной работы всего, в том числе:	58,3
в том числе:		аудиторная работа	54
аудиторные занятия	54	текущие консультации по практическим занятиям	1,8
самостоятельная работа	90	консультации перед экзаменом	2
часов на контроль	36	прием экзамена	0,5
Промежуточная аттестация и формы контроля:			
экзамен	4		

#### **Распределение часов дисциплины по семестрам**

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		Итого	
	Неделя			
Вид занятий	УП	РП	УП	РП
Лекции	36	36	36	36
Практические	18	18	18	18
Элект	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	90	90	90	90
Сам. работа	90	90	90	90
Часы на контроль	36	36	36	36
Итого	216	216	216	216

<b>1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>	
1.1	Цель дисциплины: Системно изложить современный подход к вопросам информационной безопасности и защиты информации в Российской Федерации.
1.2	Задачи дисциплины: Получение навыков системного использования и применения основных принципов и методологии построения эффективных систем защиты информации; изучение нормативных правовых документов, действующих в данной предметной области.

<b>2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП</b>	
Цикл (раздел) ОП:	Б1.Б
<b>2.1 Требования к предварительной подготовке обучающегося:</b>	
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения дисциплины Основы информационной безопасности. В результате освоения предшествующих дисциплин обучающийся должен знать: место и роль информационной безопасности в системе национальной безопасности; уметь: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; профессиональной терминологией.	
<b>2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
Безопасность информационных процессов Безопасность сетей ЭВМ Защита информации от утечки по техническим каналам Информационная безопасность телекоммуникационных систем Основы управления информационной безопасностью Защита информационных процессов на транспорте Комплексные системы защиты информации на транспорте Программно-аппаратные средства защиты информации Производственная практика (технологическая практика) Управление информационной безопасностью на объектах транспортной инфраструктуры	

<b>3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ</b>	
<b>УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач</b>	
<b>УК-1.3: Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи</b>	
<b>ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;</b>	
<b>ОПК-8.2: Анализирует и обобщает научно-техническую литературу, нормативные и методические документы для решения поставленной задачи профессиональной деятельности</b>	
<b>ОПК-8.1: Использует электронные информационные ресурсы для поиска научно-технической литературы, нормативных и методических документов в области профессиональной деятельности</b>	
<b>ОПК(п)-2.1: Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;</b>	
<b>ОПК(п)-2.1.1: Знает функциональные процессы и информационные составляющие объектов защиты</b>	
<b>ОПК(п)-2.1.2: Выявляет источники информационных угроз, их возможные цели, пути реализации</b>	
<b>ОПК(п)-2.1.3: Оценивает предполагаемый ущерб от реализации информационных угроз</b>	
<b>ОПК(п)-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;</b>	
<b>ОПК(п)-2.3.2: Знает и применяет международные и национальные стандарты в области информационной безопасности</b>	

**В результате освоения дисциплины обучающийся должен**

<b>3.1</b>	<b>Знать:</b>
3.1.1	направления обеспечения информационной безопасности государства;
3.1.2	основные термины по проблематике информационной безопасности;
3.1.3	методологию создания систем защиты информации;
3.1.4	перспективные направления развития средств и методов защиты информации;
3.1.5	роль и место информационной безопасности в системе национальной безопасности;

3.1.6	основы организационного и правового обеспечения информационной безопасности;
3.1.7	классификацию защищаемой информации; классификацию угроз защищаемой информации.
<b>3.2</b>	<b>Уметь:</b>
3.2.1	выбирать показатели качества и критерии оценки систем и средств защиты информации;
3.2.2	пользоваться современной научно-технической информацией по вопросам безопасности;
3.2.3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и модели нарушителей информационной безопасности выявлять уязвимости информационных ресурсов, проводить мониторинг угроз информационной безопасности.
<b>3.3</b>	<b>Владеть:</b>
3.3.1	навыками поиска нормативной правовой информации,необходимой для профессиональной деятельности;
3.3.2	навыками обоснования, выбора, реализации и контроля результатов управленческого решения;
3.3.3	навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;
3.3.4	навыками работы с нормативными правовыми актами.

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	<b>Раздел 1. Концептуальные понятия информационной безопасности</b>					
1.1	Закон Российской Федерации "О безопасности". Концепция национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации /Лек/	4	4	УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1 Э1 Э2	
1.2	Сущность и понятие информационной безопасности, характеристика ее составляющих. Значение информационной безопасности для субъектов информационных отношений /Пр/	4	2	ОПК(п)-2.1.1 ОПК (п)-2.1.2 ОПК(п)-2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.2 Э1 Э2	Групповая дискуссия
1.3	Федеральный закон «Об информации, информационных технологиях и о защите информации». Закон Российской Федерации «О государственной тайне» /Лек/	4	4	УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1 Э1 Э2	
1.4	Подготовка к практическим занятиям /Ср/	4	8	ОПК(п)-2.1.1 ОПК (п)-2.1.2 ОПК(п)-2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
1.5	Понятие и сущность защиты информации. Защищаемая информация – основные свойства и состав. Место защиты информации в системе информационной безопасности РФ. Классификация информации ограниченного доступа /Пр/	4	2	ОПК(п)-2.1.1 ОПК (п)-2.1.2 ОПК(п)-2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.2 Э1 Э2	Групповая дискуссия

1.6	План защиты информации на предприятии /Пр/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.2 Э1 Э2	Групповая дискуссия
1.7	Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации /Лек/	4	4	УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1 Э1 Э2	
1.8	Подготовка к практическим занятиям /Ср/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
1.9	Методологические подходы к защите информации и принципы ее организации. Объекты защиты. Виды защиты. Классификация методов и средств защиты информации /Пр/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.2 Э1 Э2	Групповая дискуссия
1.10	Изучение литературы по тематике раздела /Ср/	4	18	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
	<b>Раздел 2. Технология создания политики безопасности</b>					
2.1	Дискреционный принцип разграничения доступа /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	
2.2	Мандатный принцип разграничения доступа (нормативный) /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	
2.3	Классическая модель Бел Ла Падуды /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	
2.4	Уполномоченные субъекты в моделях, реализующих мандатный доступ /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	
2.5	Безопасная функция перехода модели совместного доступа /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	
2.6	Модель совместного доступа с уполномоченными субъектами. Ролевая политика доступа /Лек/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2	Л1.1 Л1.3Л2.1 Э1 Э2	

2.7	Подготовка к практическим занятиям /Ср/	4	4	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
2.8	Понятие и сущность защиты информации. Защищаемая информация – основные свойства и состав. Место защиты информации в системе информационной безопасности РФ. Классификация информации ограниченного доступа /Пр/	4	6	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Э1 Э2	Групповая дискуссия
2.9	Изучение литературы по тематике раздела /Ср/	4	20	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
2.10	Подготовка к промежуточной аттестации /Ср/	4	36	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
2.11	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	4	36	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	
2.12	Промежуточная аттестация /Экзамен/	4	36	ОПК(п)- 2.1.1 ОПК (п)-2.1.2 ОПК(п)- 2.1.3 ОПК (п)-2.3.2 УК-1.3 ОПК-8.1 ОПК-8.2	Л1.1 Л1.3Л2.1Л3.1 Э1 Э2	

### 5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

### 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

<b>6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)</b>				
<b>6.1.1. Основная учебная литература</b>				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Паршин К. А.	Теория информационной безопасности и методология защиты информации: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2020	<a href="http://znanium.com">http://znanium.com</a>
Л1.3	Ададуров С. Е., Глухов А. П., Иванов Д. Д., Горелик В. Ю.	Информационная безопасность и защита информации на железнодорожном транспорте. Часть 1: учебник: в 2 ч.	Москва: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2015	<a href="https://umczdt.ru/books/">https://umczdt.ru/books/</a>
<b>6.1.2. Дополнительная учебная литература</b>				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учебное пособие для студентов вузов, обучающихся по специальности 230201 - "Информационные системы и технологии"	Москва: Академия, 2009	
<b>6.1.3. Методические разработки</b>				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю., Ганженко Н. В.	Теория информационной безопасности и методология защиты информации: методические рекомендации к самостоятельной работе студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
Л3.2	Зырянова Т. Ю.	Теория информационной безопасности и методология защиты информации: методические рекомендации по подготовке к практическим семинарам для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
<b>6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)</b>				
Э1	Официальный сайт Федеральной службы по техническому и экспортному контролю Российской Федерации ( <a href="http://www.fstec.ru">http://www.fstec.ru</a> )			
Э2	Система электронной поддержки обучения Blackboard Learn ( <a href="http://bb.usurt.ru">http://bb.usurt.ru</a> )			
<b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем</b>				
<b>6.3.1 Перечень программного обеспечения</b>				
6.3.1.1	Неисключительные права на ПО Windows			
6.3.1.2	Неисключительные права на ПО Office			
6.3.1.3	Система электронной поддержки обучения Blackboard Learn			
<b>6.3.2 Перечень информационных справочных систем и профессиональных баз данных</b>				
6.3.2.1	Справочно-правовая система КонсультантПлюс			
6.3.2.2	Справочно-правовая система Гарант			
6.3.2.3	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)			
6.3.2.4	Банк данных угроз безопасности информации ФСТЭК России: <a href="https://bdu.fstec.ru/">https://bdu.fstec.ru/</a>			

<b>7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)</b>	
Назначение	Оснащение
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Компьютерный класс - Учебная аудитория для самостоятельной работы студентов	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования

<b>8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)</b>
<p>Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком. Обучающемуся рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонифицированную электронную карту и уметь пользоваться электронным каталогом «ИРБИС»). Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети «Интернет» организован в читальных залах библиотеки, в компьютерных классах, в помещениях для самостоятельной работы обучающихся со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи. Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий. Комплект учебно-методических материалов по всем видам учебной деятельности, предусмотренной рабочей программой дисциплины (модуля), размещен на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося. Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя: - изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий); - подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполняя самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)". Перечень учебно-методических материалов (учебно-методического обеспечения) для самостоятельной работы обучающихся по дисциплине указан по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)", материалы размещены на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru).</p> <p>При применении дистанционных образовательных технологий и электронного обучения освоение дисциплины (модуля)</p>

осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт [bb.usurt.ru](http://bb.usurt.ru))) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.