

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение высшего  
образования «Вятский государственный университет»  
(ВятГУ)  
г. Киров

Утверждаю  
Директор/Декан Репкин Д. А.



Номер регистрации  
РПД\_3-10.05.02.01\_2017\_82136  
Актуализировано: 27.04.2021

**Рабочая программа дисциплины**  
**Безопасность функционирования информационных систем**

	наименование дисциплины
Квалификация выпускника	Специалист по защите информации
Специальность	10.05.02
	шифр
	Информационная безопасность телекоммуникационных систем
	наименование
Специализация	Системы подвижной цифровой защищенной связи
	наименование
Формы обучения	Очная
	наименование
Кафедра-разработчик	Кафедра радиоэлектронных средств
	наименование
Выпускающая кафедра	Кафедра радиоэлектронных средств
	наименование

## Сведения о разработчиках рабочей программы дисциплины

Трубин Игорь Сергеевич

---

ФИО

## Цели и задачи дисциплины

Цель дисциплины	Целью преподавания дисциплины является сформировать у обучающихся систематизированный подход к обеспечению безопасного функционирования информационных систем на всех стадиях жизненного цикла
Задачи дисциплины	<p>К основным задачам курса относятся:</p> <ul style="list-style-type: none"> <li>- изучение архитектуры безопасности эталонной модели взаимодействия открытых систем (ЭМВОС/OSI);</li> <li>- раскрытие особенностей реализации системы защиты информации как основы обеспечения ИБ на всех стадиях жизненного цикла ИС;</li> <li>- формирование у обучаемых целостного представления о характеристиках и параметрах безопасности функционирования ИС организации;</li> <li>- изучение базовых технологий обеспечения информационной безопасности;</li> <li>- получение навыков рационального выбора средств и методов защиты информации в ИС;</li> <li>- получение навыков корпоративной защиты информации от внутренних угроз.</li> </ul>

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

#### Компетенция ПК-7

способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования		
Знает	Умеет	Владеет
- принципы построения и функционирования информационных систем (ИС), методы доступа, типы физической среды передачи данных в ИС; - основные стандарты, стеки протоколов и интерфейсы, используемые в ИС; - сетевые операционные системы ИС.	- выбрать тип физической среды передачи данных в ИС, технологию доступа; - анализировать стандарты, стеки протоколов и интерфейсы, используемые в ИС; - организовывать и поддерживать выполнение комплекса мер по информационной безопасности ИС с учетом предъявляемых к ним требований качества обслуживания и качества функционирования.	- основными стандартами, протоколами, интерфейсами ИС; - готовностью конфигурирования ИС, реализации сетевых протоколов с помощью программных средств; - способностью выбирать методы и средства обеспечения информационной безопасности ИС.

#### Компетенция ПК-9

способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации		
Знает	Умеет	Владеет

<p>- основные компоненты информационных систем (ИС); - методы анализа и построения защиты локальных внутренних и распределенных внешних вычислительных и информационных сетей предприятия; - основы построения систем защиты информации в ИС; - принципы аттестации телекоммуникационных систем по требованиям защиты информации.</p>	<p>- эффективно использовать различные методы и средства защиты информации в ИС; - использовать встроенные возможности аппаратных и программных ресурсов ИС для обеспечения информационной безопасности; - осуществлять рациональный выбор средств и методов защиты информации в ИС; - участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации.</p>	<p>- готовностью внедрять программно-аппаратные средства обеспечения информационной безопасности ИС; - современными методами и средствами защиты информации в ИС; - способностью выбора современного телекоммуникационного оборудования и средств защиты информации ИС; - способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации.</p>
---	--	--

### Компетенция ПК-15

<p>способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания</p>		
<p><b>Знает</b></p>	<p><b>Умеет</b></p>	<p><b>Владеет</b></p>
<p>- эволюцию развития и классификацию ИС, основные типы сетевых топологий; - виды и формы информации, наиболее подверженной угрозам в ИС; - источники и классификацию угроз информационной безопасности в ИС; - основные уязвимости технологий и программно-аппаратных компонентов ИС; - технологии, средства и методы обеспечения информационной безопасности ИС; - требования к качеству обслуживания и защищенности ИС.</p>	<p>- анализировать и оценивать угрозы информационной безопасности ИС; - оценивать уязвимость протоколов и интерфейсов ИС; - определять виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов в ИС предприятия, целей и задач деятельности предприятия; - выбирать и оценивать архитектуру защищенной ИС и ее подсистем; - анализировать информационную безопасность функционирования ИС; - проводить инструментальный мониторинг защищенности ИС, обеспечения требуемого качества обслуживания.</p>	<p>- готовностью прогнозировать, ранжировать, анализировать угрозы ИС; - умением оценивать уровни риска ИС; - способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов в ИС предприятия, целей и задач деятельности предприятия; - методологией анализа защищенности информационной системы; - способностью выявлять тенденции развития информационной безопасности ИС; - способностью проводить инструментальный</p>

		мониторинг защищенности ИС, обеспечения требуемого качества обслуживания.
--	--	---

**Структура дисциплины**  
**Тематический план**

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	ИКС как среда для обработки, хранения и передачи информации	ПК-9
2	Архитектура безопасности ЭМВОС	ПК-7
3	Уязвимости, атаки и последствия атак на ИКС	ПК-15
4	Моделирование параметров и характеристик безопасности	ПК-15
5	Система защиты информации как основа безопасного функционирования ИС	ПК-9
6	Подготовка и прохождение промежуточной аттестации	ПК-15, ПК-7, ПК-9

**Формы промежуточной аттестации**

Зачет	Не предусмотрен (Очная форма обучения)
Экзамен	8 семестр (Очная форма обучения)
Курсовая работа	Не предусмотрена (Очная форма обучения)
Курсовой проект	Не предусмотрена (Очная форма обучения)

### Трудоемкость дисциплины

Форма обучения	Курсы	Семестры	Общий объем (трудоемкость)		Контактная работа, час	в том числе аудиторная контактная работа обучающихся с преподавателем, час				Самостоятельная работа, час	Курсовая работа (проект), семестр	Зачет, семестр	Экзамен, семестр
			Часов	ЗЕТ		Всего	Лекции	Семинарские, практические занятия	Лабораторные занятия				
Очная форма обучения	4	8	144	4	68.5	36	18	0	18	75.5			8

## Содержание дисциплины

### Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
<b>Раздел 1 «ИКС как среда для обработки, хранения и передачи информации»</b>		<b>18.00</b>
<b>Лекции</b>		
Л1.1	Цели и задачи курса	0.50
Л1.2	ИКС как среда для обработки, хранения и передачи информации	1.00
Л1.3	Жизненный цикл ИКС	0.25
Л1.4	Понятие эксплуатационной безопасности	0.25
<b>Лабораторные занятия</b>		
Р1.1	Установка и конфигурирование компонентов DLP системы	6.00
<b>Самостоятельная работа</b>		
С1.1	ИКС как среда для обработки, хранения и передачи информации (проработка материалов лекции Л1.2)	2.00
С1.2	Изучение документации InfoWatch ТМ (подготовка к лабораторной работе Р1.1)	4.00
<b>Контактная внеаудиторная работа</b>		
КВР1.1	Контактная внеаудиторная работа	4.00
<b>Раздел 2 «Архитектура безопасности ЭМВОС»</b>		<b>18.00</b>
<b>Лекции</b>		
Л2.1	Распределение механизмов и услуг безопасности по уровням архитектуры ЭМВОС	1.00
Л2.2	Принципы архитектуры безопасности сети Интернет	1.00
<b>Лабораторные занятия</b>		
Р2.1	Изучение структуры InfoWatch ТМ и DM	4.00
<b>Самостоятельная работа</b>		
С2.1	Изучение документации InfoWatch ТМ (подготовка к лабораторной работе Р2.1)	4.00
С2.2	Архитектура безопасности ЭМВОС (проработка материалов лекции Л2.1 - Л2.2)	2.00
<b>Контактная внеаудиторная работа</b>		
КВР2.1	Контактная внеаудиторная работа	6.00
<b>Раздел 3 «Уязвимости, атаки и последствия атак на ИКС»</b>		<b>26.00</b>
<b>Лекции</b>		
Л3.1	Угрозы уязвимостей и уровни защиты (защищенности)	1.00
Л3.2	Стадии реализации атаки	1.00
Л3.3	Моделирование уязвимостей реализации и атак	1.00
Л3.4	Жизненный цикл типовой информационные атаки на ресурсы ИКС	0.50
Л3.5	Метрики защиты CVSS (Common Vulnerability Scoring System)	0.50



Л3.6	Обеспечение безопасности сетей ОКС-7	2.00
<b>Лабораторные занятия</b>		
Р3.1	Технологии агентского мониторинга в InfoWatchn TM	2.00
Р3.2	Механизмы диагностики агента, подходы к защите агента InfoWatch DM	2.00
<b>Самостоятельная работа</b>		
С3.1	Изучение документации InfoWatch TM (подготовка к лабораторным работам Р3.1 и Р3.2)	4.00
С3.2	Методика расчета метрик CVSS 2.0 и 3.0 (проработка материалов лекции Л3.5 )	4.00
С3.3	Стадии жизненного цикла информационной атаки на ресурсы ИКС (проработка материалов лекции Л3.4)	2.00
С3.4	Стадии реализации атаки (проработка материалов лекции Л3.2 - Л3.3)	2.00
<b>Контактная внеаудиторная работа</b>		
КВР3.1	Контактная внеаудиторная работа	4.00
<b>Раздел 4 «Моделирование параметров и характеристик безопасности»</b>		<b>16.00</b>
<b>Лекции</b>		
Л4.1	Моделирование параметров и характеристик безопасности	1.00
Л4.2	Угроза безопасности как объект моделирования	1.00
Л4.3	Марковская модель угрозы безопасности	0.50
Л4.4	Оценка актуальности угроз атак	1.00
Л4.5	Функциональная модель потенциального нарушителя	0.50
<b>Самостоятельная работа</b>		
С4.1	Угроза безопасности как объект моделирования (проработка материалов лекций Л4.1 - 4.5)	2.00
С4.2	Функциональная модель потенциального нарушителя (проработка материалов лекции Л4.5)	2.00
<b>Контактная внеаудиторная работа</b>		
КВР4.1	Контактная внеаудиторная работа	8.00
<b>Раздел 5 «Система защиты информации как основа безопасного функционирования ИС »</b>		<b>30.00</b>
<b>Лекции</b>		
Л5.1	Концепция обеспечения ИБ	0.50
Л5.2	Основные функции СЗИ	0.25
Л5.3	Средства обеспечения ИБ	0.50
Л5.4	Службы обеспечения информационной безопасности	0.50
Л5.5	Участники обеспечения ИБ	0.25
Л5.6	Базовые технологии обеспечения информационной безопасности	2.00
<b>Лабораторные занятия</b>		
Р5.1	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	4.00
<b>Самостоятельная работа</b>		
С5.1	Изучение документации InfoWatch TM (подготовка к	4.00

	лабораторной работе Р5.1)	
С5.2	Основы аутентификации (проработка материалов лекции Л5.6)	3.00
С5.3	Технология межсетевого экранирования (проработка материалов лекции Л5.6)	3.00
С5.4	Концепция обеспечения ИБ (проработка материалов лекций Л5.1 - Л5.4)	4.00
<b>Контактная внеаудиторная работа</b>		
КВР5.1	Контактная внеаудиторная работа	8.00
<b>Раздел 6 «Подготовка и прохождение промежуточной аттестации»</b>		<b>36.00</b>
Э6.1	Подготовка к сдаче экзамена	33.50
КВР6.1	Консультация перед экзаменом	2.00
КВР6.2	Сдача экзамена	0.50
<b>ИТОГО</b>		<b>144.00</b>

Содержание дисциплины данной рабочей программы используется при обучении по индивидуальному учебному плану, при ускоренном обучении, при применении дистанционных образовательных технологий и электронном обучении (при наличии).

## Методические указания для обучающихся по освоению дисциплины

Успешное освоение дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции, семинарские, практические и лабораторные занятия (при их наличии), получать консультации преподавателя и выполнять самостоятельную работу.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Тематика лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов.

Предполагается, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендованным программой. Часто обучающимся трудно разобраться с дискуссионными вопросами, дать однозначный ответ. Преподаватель, сравнивая различные точки зрения, излагает свой взгляд и нацеливает их на дальнейшие исследования и поиск научных решений. После лекции желательно вечером перечитать и закрепить полученную информацию, тогда эффективность ее усвоения значительно возрастает. При работе с конспектом лекции необходимо отметить материал, который вызывает затруднения для понимания, попытаться найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю.

Целью семинарских занятий является проверка уровня понимания обучающимися вопросов, рассмотренных на лекциях и в учебной литературе.

Целью практических и лабораторных занятий является формирование у обучающихся умений и навыков применения теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса.

Семинарские, практические и лабораторные занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Для успешного участия в семинарских, практических и лабораторных занятиях обучающемуся следует тщательно подготовиться.

Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и т.п.

Изучив конкретную тему, обучающийся может определить, насколько хорошо он в ней разобрался. Если какие-то моменты остались непонятными, целесообразно составить список вопросов и на занятии задать их преподавателю. Практические (лабораторные) занятия предоставляют обучающемуся возможность творчески раскрыться, проявить инициативу и развить навыки публичного ведения дискуссий и общения.

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий (изучение учебной и научной литературы, материалов лекций, систематизацию прочитанного материала, подготовку контрольной работы, решение

задач, подготовка докладов, написание рефератов, публикация тезисов, научных статей, подготовка и защита курсовой работы / проекта и другие), которые ориентированы на глубокое усвоение материала изучаемой дисциплины.

Обучающимся рекомендуется систематически отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки.

Внутренняя система оценки качества освоения дисциплины включает входной контроль уровня подготовленности обучающихся, текущий контроль успеваемости, промежуточную аттестацию, направленную на оценивание промежуточных и окончательных результатов обучения по дисциплине (в том числе результатов курсового проектирования (выполнения курсовых работ) при наличии).

При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля, проводимого в течение освоения дисциплины.

Процедура оценивания результатов освоения дисциплины осуществляется на основе действующих локальных нормативных актов ФГБОУ ВО «Вятский государственный университет», с которыми обучающиеся знакомятся на официальном сайте университета [www.vyatsu.ru](http://www.vyatsu.ru).

## **Учебно-методическое обеспечение дисциплины, в том числе учебно-методическое обеспечение самостоятельной работы обучающегося по дисциплине**

### **Учебная литература (основная)**

1) Смирнова, Е. В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных : учеб. пособие / Е. В. Смирнова, П. В. Козик ; ред. Б. В. Костров. - СПб. : БХВ-Петербург, 2012. - 271, [1] с. - Библиогр. в конце кн. - ISBN 978-5-9775-0831-5 : 293.00 р. - Текст : непосредственный.

2) Васин, Николай Николаевич. Основы сетевых технологий на базе коммутаторов и маршрутизаторов : учеб. пособие / Н. Н. Васин. - Москва : Интернет-Ун-т Информ. Технологий : Бинум. Лаборатория знаний, 2011. - 270 с. : ил., табл. - (Основы информационных технологий). - Библиогр.: с. 253. - ISBN 978-5-9963-0489-9 : 287.50 р. - Текст : непосредственный.

3) Грибунин, Вадим Геннадьевич. Комплексная система защиты информации на предприятии : учеб. пособие для студентов высших учебных заведений, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации" направления подготовки "Информационная безопасность" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 411, [1] с. : ил. ; 22. - (Высшее профессиональное образование. Информационная безопасность) (Учебное пособие). - Библиогр.: с. 403-406 (52 назв.). - 2500 экз. - ISBN 978-5-7695-5448-3 : 425.70 р. - Текст : непосредственный.

4) Бондарев, Е. С. Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. - Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. - 146 с. - ISBN 978-5-907054-82-0 : Б. ц. - URL: <https://e.lanbook.com/book/157086> (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

5) Богатырев, Владимир Анатольевич. Информационные системы и технологии. Теория надежности : Учебное пособие для вузов / В. А. Богатырев. - Москва : Юрайт, 2020. - 318 с. - (Высшее образование). - ISBN 978-5-534-00475-5 : 769.00 р. - URL: <https://urait.ru/bcode/451108> (дата обращения: 08.05.2020). - Режим доступа: Образовательная платформа Юрайт. - Текст : электронный.

6) Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. - Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=480637/> (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

7) Петровский, В. И. Принципы построения системы защиты информации на предприятиях различных форм собственности : учебное пособие / В. И. Петровский. - Казань : КНИТУ-КАИ, 2016. - 512 с. - ISBN 978-5-7579-2150-1 : Б. ц. -

URL: <https://e.lanbook.com/book/149575> (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

8) Мельников, Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студ. вузов, обучающихся по спец. "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 6-е изд., стер. - М. : Академия, 2012. - 336 с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5 : 422.40 р. - Текст : непосредственный.

9) Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6 : Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=253553/> (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

10) Шаньгин, Владимир Федорович. Комплексная защита информации в корпоративных системах : учеб. пособие для студентов высших учебных заведений, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : Форум : ИНФРА-М, 2010. - 591 с. : ил. ; 24. - (Высшее образование). - Предм. указ.: с. 574-584. - Библиогр.: с. 568-573. - ISBN 978-5-8199-0411-4 ФОРУМ. - ISBN 978-5-16-003746-2 ИНФРА-М : 509.60 р. - Текст : непосредственный.

#### **Учебная литература (дополнительная)**

1) Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 : Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=93351/> (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Аджемов, Александр Сергеевич. Система сигнализации ОКС N7 / А. С. Аджемов, А. Е. Кучерявый. - М. : Радио и связь, 2002. - 368 с. : ил. - Библиогр.: с. 353. - ISBN 5-256-0634-2 : 257.40 р. - Текст : непосредственный.

3) Общекабельная сигнализация ОКС №7 : метод. указание к лабор. работе по курсу "АТС городских и сельских сетей связи" / ВятГУ, ФПМТ, каф.РЭС ; сост. Д. Е. Прозоров. - Киров : ВятГУ, 2009. - х. - Б. ц. - URL: <https://lib.vyatsu.ru>. - Режим доступа: для авториз. пользователей. - Текст : электронный.

4) Скрипник, Д. А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. - Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=429070/> (дата обращения:

24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

5) Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко. - Ставрополь : СКФУ, 2015. - 222 с. - Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=458204/> (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

6) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. | Берлин : Директ-Медиа, 2015. - 253 с. - ISBN 978-5-4475-3946-7 : Б. ц. - URL: <http://biblioclub.ru/index.php?page=book&id=276557/> (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

### **Электронные образовательные ресурсы**

- 1) Портал дистанционного обучения ВятГУ [электронный ресурс] / - Режим доступа: <http://mooc.do-kirov.ru/>
- 2) Раздел официального сайта ВятГУ, содержащий описание образовательной программы [электронный ресурс] / - Режим доступа: [https://www.vyatsu.ru/php/programms/eduPrograms.php?Program\\_ID=3-10.05.02.01](https://www.vyatsu.ru/php/programms/eduPrograms.php?Program_ID=3-10.05.02.01)
- 3) Личный кабинет студента на официальном сайте ВятГУ [электронный ресурс] / - Режим доступа: <https://new.vyatsu.ru/account/>
- 4) Единое окно доступа к образовательным ресурсам <http://window.edu.ru/>

### **Электронные библиотечные системы (ЭБС)**

- ЭБС «Научная электронная библиотека eLIBRARY» (<http://elibrary.ru/defaultx.asp>)
- ЭБС «Издательства Лань» (<http://e.lanbook.com/>)
- ЭБС «Университетская библиотека online» ([www.biblioclub.ru](http://www.biblioclub.ru))
- Внутренняя электронно-библиотечная система ВятГУ (<http://lib.vyatsu.ru/>)
- ЭБС «ЮРАЙТ» (<https://urait.ru>)

### **Современные профессиональные базы данных и информационные справочные системы**

- ГАРАНТ
- КонсультантПлюс
- Техэксперт: Нормы, правила, стандарты
- Роспатент (<https://www1.fips.ru/elektronnye-servisy/informatsionno-poiskovaya-sistema>)
- Web of Science® (<http://webofscience.com>)

## Материально-техническое обеспечение дисциплины

### Демонстрационное оборудование

Перечень используемого оборудования
ИНТЕРАКТИВНАЯ ДОСКА SMART BOARD 480IV СО ВСТРОЕННЫМ ПРОЕКТОРОМ V25 С КАБЕЛЕМ VGA 15,2М C-GM/GM-50

### Специализированное оборудование

Перечень используемого оборудования
КОММУТАТОР Catalyst 2960 24
МАРШРУТИЗАТОР C1921
МАРШРУТИЗАТОР Cisco 2901
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL SafeRay S251.Mi (МОНОБЛОК)
ТОЧКА БЕСПРОВОДНОГО ДОСТУПА ЛВС Cisco AIRONET 1600
ШКАФ ТЕЛЕКОММУНИКАЦИОННЫЙ НАПОЛЬНЫЙ 19" (600x1020x2030)

### Учебно-наглядное пособие

Перечень используемого оборудования
МЕЖСЕТЕВОЙ ЭКРАН Cisco ASA 5505



**Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе лицензионное и свободно распространяемое ПО (включая ПО отечественного производства)**

№ п.п	Наименование ПО	Краткая характеристика назначения ПО
1	Программная система с модулями для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»	Программный комплекс для проверки текстов на предмет заимствования из Интернет-источников, в коллекции диссертация и авторефератов Российской государственной библиотеки (РГБ) и коллекции нормативно-правовой документации LEXPRO
2	Microsoft Office 365 ProPlusEdu ALNG SubsVL MVL AddOn toOPP	Набор веб-сервисов, предоставляющий доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами
3	Office Professional Plus 2016	Пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных, презентациями
4	Windows Professional	Операционная система
5	Kaspersky Endpoint Security для бизнеса	Антивирусное программное обеспечение
6	Справочная правовая система «Консультант Плюс»	Справочно-правовая система по законодательству Российской Федерации
7	Электронный периодический справочник ГАРАНТ Аналитик	Справочно-правовая система по законодательству Российской Федерации
8	Security Essentials (Защитник Windows)	Защита в режиме реального времени от шпионского программного обеспечения, вирусов.
9	МойОфис Стандартный	Набор приложений для работы с документами, почтой, календарями и контактами на компьютерах и веб браузерах
10	2019 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ InfoWatch Traffic Monitor Education Lab Extended бессрочная лицензия на 16 серверов	Специализированное лицензионное ПО

Обновленный список программного обеспечения данной рабочей программы находится по адресу:  
[https://www.vyatsu.ru/php/list\\_it/index.php?op\\_id=82136](https://www.vyatsu.ru/php/list_it/index.php?op_id=82136)

