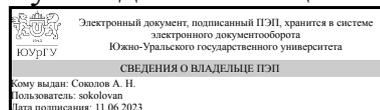


УТВЕРЖДАЮ:  
Руководитель специальности



А. Н. Соколов

## РАБОЧАЯ ПРОГРАММА

**дисциплины 1.О.45 Основы технической эксплуатации значимых объектов критической информационной инфраструктуры для специальности 10.05.03 Информационная безопасность автоматизированных систем**

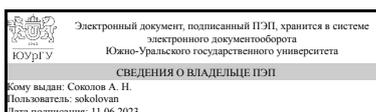
**уровень** Специалитет

**форма обучения** очная

**кафедра-разработчик** Защита информации

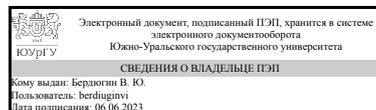
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

Зав.кафедрой разработчика,  
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,  
доцент



В. Ю. Бердюгин

## 1. Цели и задачи дисциплины

Целью преподавания дисциплины является знакомство студентов с принципами, особенностями и способами обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры. Задачами дисциплины являются: - изучение системы государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; - обучение принципам анализа с целью выявления потенциальных уязвимостей безопасности значимых объектов критической информационной инфраструктуры; - выработка умений классифицировать и оценивать угрозы безопасности значимых объектов критической информационной инфраструктуры, эффективно использовать различные методы и средства защиты информации; - изучение основных средств и способов обеспечения безопасности значимых объектов критической информационной инфраструктуры, принципов построения систем защиты информации.

## Краткое содержание дисциплины

Основные направления государственной политики в области обеспечения безопасности объектов критической инфраструктуры Российской Федерации. Особенности обеспечения информационной безопасности на различных этапах жизненного цикла объектов критической информационной инфраструктуры. Силы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-18 (11.2) Способен обеспечивать функционирование систем безопасности значимых объектов критической информационной инфраструктуры	Знает: требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры; программно-аппаратные средства защиты информации, входящие в состав систем безопасности значимых объектов критической информационной инфраструктуры; способы и методы эксплуатации автоматизированных систем в защищенном исполнении при обеспечении безопасности значимых объектов критической информационной инфраструктуры Умеет: обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»; обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и эксплуатацию средств защиты информации; готовить предложения по совершенствованию

	<p>функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры</p> <p>Имеет практический опыт: технической эксплуатации средств защиты информации при обеспечении безопасности значимых объектов критической информационной инфраструктуры</p>
--	---

### 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		10
Общая трудоёмкость дисциплины	144	144
<i>Аудиторные занятия:</i>	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	69,5	69,5
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 3).	25,5	25,5
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 2).	24	24
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 1).	20	20
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

### 5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах
-----------	----------------------------------	---

		Всего	Л	ПЗ	ЛР
1	Основные направления государственной политики в области обеспечения безопасности объектов критической инфраструктуры Российской Федерации	16	8	8	0
2	Особенности обеспечения информационной безопасности на различных этапах жизненного цикла объектов критической информационной инфраструктуры	20	10	10	0
3	Силы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.	28	14	14	0

## 5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие критической информационной инфраструктуры Российской Федерации (КИИ РФ). Перечень показателей критериев значимости объектов КИИ РФ.	2
2	1	Организационные основы обеспечения информационной безопасности КИИ РФ.	2
3	1	Права и обязанности субъектов КИИ. Государственный контроль и надзор в области обеспечения безопасности объектов КИИ.	2
4	1	Ответственность за нарушение требований обеспечения безопасности значимых объектов КИИ.	2
5	2	Перечень показателей критериев значимости объектов КИИ. Порядок категорирования объектов КИИ.	2
6	2	Стадии жизненного цикла безопасности объектов КИИ.	2
7	2	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.	2
8	2	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ.	2
9	2	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ.	2
10	3	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.	2
11	3	Политики обеспечения безопасности значимых объектов КИИ.	2
12	3	Программно-технические средства обеспечения безопасности значимых объектов КИИ.	2
13	3	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.	2
14	3	Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак.	2
15	3	Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.	2
16	3	Порядок реагирования и обмена информацией о компьютерных инцидентах между субъектами КИИ РФ.	2

## 5.2. Практические занятия, семинары

№	№	Наименование или краткое содержание практического занятия, семинара	Кол-
---	---	---	------

занятия	раздела		во часов
1	1	Понятие критической информационной инфраструктуры Российской Федерации (КИИ РФ). Перечень показателей критериев значимости объектов КИИ РФ и их значения.	2
2	1	Организационные основы обеспечения информационной безопасности КИИ РФ.	2
3	1	Права и обязанности субъектов КИИ. Государственный контроль и надзор в области обеспечения безопасности объектов КИИ.	2
4	1	Ответственность за нарушение требований обеспечения безопасности значимых объектов КИИ.	2
5-6	2	Перечень показателей критериев значимости объектов КИИ. Порядок категорирования объектов КИИ. Стадии жизненного цикла безопасности объектов КИИ.	4
7	2	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.	2
8	2	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ.	2
9	2	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ.	2
10	3	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.	2
11-12	3	Политики обеспечения безопасности значимых объектов КИИ. Программно-технические средства обеспечения безопасности значимых объектов КИИ.	4
13	3	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.	2
14	3	Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак.	2
15	3	Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.	2
16	3	Порядок реагирования и обмена информацией о компьютерных инцидентах между субъектами КИИ РФ.	2

### 5.3. Лабораторные работы

Не предусмотрены

### 5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 3).	1. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 3. Кибербезопасность электроэнергетических инфраструктур.. 3. Лекции преподавателя (стр. 30-37, 42-	10	25,5

	45).		
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 2).	1. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 3. Кибербезопасность электроэнергетических инфраструктур. 2. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020, Глава 5. Основы поиска уязвимостей программного обеспечения. 3. Лекции преподавателя (стр. 27-30, 37-42).	10	24
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 1).	1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020, Глава 1. Теоретические основы информационной безопасности. 2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 3. Кибербезопасность электроэнергетических инфраструктур. 3. Лекции преподавателя (стр. 15-22).	10	20

## 6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

### 6.1. Контрольные мероприятия (КМ)

№ КМ	Се- местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи- тыва- ется в ПА
1	10	Текущий контроль	Выступление с докладом на семинаре (раздел 1)	3	9	За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от	экзамен

					<p>24.05.2019 г. № 179).</p> <p>Критерии оценки качества доклада.</p> <p>1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов.</p> <p>2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов.</p> <p>3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов.</p> <p>4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0.</p> <p>5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0.</p> <p>6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p>		
2	10	Текущий контроль	Тестирование (раздел 1)	2	10	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом	экзамен

					<p>ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p>		
3	10	Текущий контроль	Выступление с докладом на семинаре (раздел 2)	3	9	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179).</p> <p>Критерии оценки качества доклада.</p> <p>1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов.</p> <p>2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов.</p> <p>3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов.</p> <p>4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0.</p> <p>5. Качество презентации: презентация содержит не только текстовые, но и</p>	экзамен

					<p>графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл;</p> <p>презентация отсутствует – 0.</p> <p>6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл; докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p>		
4	10	Текущий контроль	Тестирование (раздел 2)	2	10	<p>При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p>	экзамен
5	10	Текущий контроль	Выступление с докладом на семинаре (раздел 3)	3	9	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179).</p> <p>Критерии оценки качества доклада.</p> <p>1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов.</p> <p>2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в</p>	экзамен

					<p>разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов.</p> <p>3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов.</p> <p>4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0.</p> <p>5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0.</p> <p>6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p>		
6	10	Текущий контроль	Тестирование (раздел 3)	2	10	<p>При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p>	экзамен
7	10	Промежуточная аттестация	Экзамен	-	12	<p>На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и</p>	экзамен

					<p>промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179)</p> <p>Студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает. Показатели оценивания ответов по каждому из вопросов: 6 баллов – студент обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы 5 баллов – студент знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. 3 балла – студент знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности 0 баллов – студент не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.</p>	
--	--	--	--	--	--	--

## 6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	При оценивании результатов учебной деятельности студента по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). В процессе проведения экзамена студенты в аудитории	В соответствии с пп. 2.5, 2.6 Положения

	письменно отвечают на вопросы билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает.	
--	---	--

### 6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ОПК-18	Знает: требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры; программно-аппаратные средства защиты информации, входящие в состав систем безопасности значимых объектов критической информационной инфраструктуры; способы и методы эксплуатации автоматизированных систем в защищенном исполнении при обеспечении безопасности значимых объектов критической информационной инфраструктуры	+	+	+	+	+	+	+
ОПК-18	Умеет: обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»; обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и эксплуатацию средств защиты информации; готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры	+	+		+	+	+	+
ОПК-18	Имеет практический опыт: технической эксплуатации средств защиты информации при обеспечении безопасности значимых объектов критической информационной инфраструктуры	+	+	+	+	+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

а) *основная литература:*

Не предусмотрена

б) *дополнительная литература:*

Не предусмотрена

в) *отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:*

Не предусмотрены

г) *методические указания для студентов по освоению дисциплины:*

1. Лекции преподавателя

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

1. Лекции преподавателя

### Электронная учебно-методическая документация

№	Вид	Наименование	Библиографическое описание
---	-----	--------------	----------------------------

	литературы	ресурса в электронной форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. <a href="https://e.lanbook.com/book/167606">https://e.lanbook.com/book/167606</a>
2	Основная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. <a href="https://e.lanbook.com/book/148386">https://e.lanbook.com/book/148386</a>
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2017. — 338 с <a href="https://e.lanbook.com/book/111049">https://e.lanbook.com/book/111049</a>
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. [Электронный ресурс] — Электрон. дан. — М. : Горячая линия-Телеком, 2015. — 586 с. <a href="https://e.lanbook.com/book/94555">https://e.lanbook.com/book/94555</a>

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

## 8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт. ), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+
Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт. ), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+