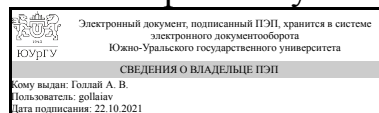


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Директор института  
Высшая школа электроники и  
компьютерных наук



А. В. Голлай

## РАБОЧАЯ ПРОГРАММА

дисциплины ДВ.1.04.02 Технологии защиты информации значимых объектов критической информационной инфраструктуры для специальности 10.05.03 Информационная безопасность автоматизированных систем

**уровень** специалист **тип программы** Специалитет

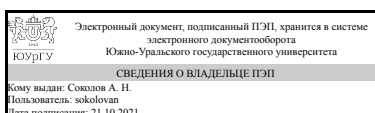
**специализация** Информационная безопасность автоматизированных систем критически важных объектов

**форма обучения** очная

**кафедра-разработчик** Защита информации

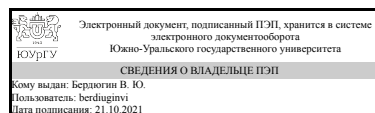
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,  
доцент



В. Ю. Бердюгин

## 1. Цели и задачи дисциплины

### Краткое содержание дисциплины

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

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать: основные информационные технологии, используемые в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	Уметь: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации
	Владеть:
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать: методы, способы, средства защиты информации в различных сферах деятельности
	Уметь: использовать стандартные методы и средства проектирования средств защиты информации
	Владеть: профессиональной терминологией в области защиты информации в различных сферах деятельности
ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Знать: средства защиты информации для обеспечения безопасности информационных систем критически важных объектов
	Уметь: выбирать средства для обеспечения безопасности информационных систем критически важных объектов
	Владеть: навыками разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня.
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать: основы правового обеспечения информационной безопасности; основные нормативные правовые акты в области обеспечения информационной безопасности
	Уметь: применять средства юридической защиты информации ограниченного доступа
	Владеть:

## 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
ДВ.1.05.02 Защита информации в автоматизированных системах управления, Б.1.24.02 Правовое обеспечение информационной безопасности	Не предусмотрены

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

Дисциплина	Требования
Б.1.24.02 Правовое обеспечение информационной безопасности	Знать: правовое обеспечение защиты информации
ДВ.1.05.02 Защита информации в автоматизированных системах управления	Знать: основные способы и методы защиты информации в автоматизированных информационных системах

#### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		10	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	60	60	
Лекции (Л)	24	24	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	48	48	
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 2)	16	16	
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 3)	16	16	
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 1)	16	16	
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет	

#### 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	12	6	6	0
2	Особенности обеспечения информационной безопасности на различных этапах жизненного цикла объектов критической информационной инфраструктуры	26	10	16	0
3	Силы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.	22	8	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 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	2	Перечень показателей критериев значимости объектов объектов КИИ. Порядок категорирования объектов КИИ.	2
5	2	Стадии жизненного цикла безопасности объектов КИИ.	2
6	2	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.	2
7	2	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ.	2
8	2	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ.	2
9	3	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.	2
10	3	Политики обеспечения безопасности значимых объектов КИИ.	2
11	3	Программно-технические средства обеспечения безопасности значимых объектов КИИ.	2
12	3	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.	2

## 5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-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
4-5	2	Перечень показателей критериев значимости объектов объектов КИИ. Порядок категорирования объектов КИИ.	4
6-7	2	Стадии жизненного цикла безопасности объектов КИИ.	4
8	2	Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.	2
9-10	2	Анализ угроз безопасности информации и разработка модели угроз безопасности объектов КИИ.	4
11	2	Планирование и разработка мероприятий по обеспечению безопасности значимых объектов КИИ.	2
12	3	Силы обеспечения безопасности значимых объектов КИИ. Порядок взаимодействия с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.	2

13-14	3	Политики обеспечения безопасности значимых объектов КИИ.	4
15-16	3	Программно-технические средства обеспечения безопасности значимых объектов КИИ.	4
17-18	3	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.	4

### 5.3. Лабораторные работы

Не предусмотрены

### 5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	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 2. Кибероружие - классификация средств и методов применения. 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 3. Политика информационной безопасности. 3. Лекции преподавателя. Теория информационной безопасности и методология защиты информации, конспект (стр. 65 - 72 )	16
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 2)	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 5. Основы поиска уязвимостей программного обеспечения. 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. Теория информационной безопасности и методология защиты информации, конспект (стр. 96 - 103)	16
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.	16

	Теоретические основы информационной безопасности. 2. Лекции преподавателя. Теория информационной безопасности и методология защиты информации, конспект (стр. 59-65)	
--	--	--

## 6. Инновационные образовательные технологии, используемые в учебном процессе

Не предусмотрены

## Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

## 7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

### 7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Тестирование	1
Все разделы	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Выступление с докладом на практических занятиях	2
Все разделы	ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Зачет	3
Все разделы	ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Выступление с докладом на практических занятиях	2
Все разделы	ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	Бонусное задание	4

### 7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Тестирование	<p>По окончании изучения каждого раздела дисциплины проводится тестирование, в процессе которого студентам предлагается выбрать правильный ответ на вопросы из предложенного перечня. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10. Весовой коэффициент - 1.</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>
Выступление с докладом на практических занятиях	<p>За неделю до семинарского занятия группе задается перечень тем (8-10) для выступления. Время, отведенное на каждое выступление, 10-15 минут. Тезисы доклада и презентация представляются в виде отчета в Электронный ЮУрГУ. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Соответствие заданию, знание нормативно-правовой базы: 2 балла – полное соответствие заданию, все ссылки на нормативно-правовые документы корректны; 2 балл – в целом соответствие заданию, однако имеются ссылки на утратившие актуальность нормативно-правовые документы; 0 баллов – не соответствие заданию; 2. Качество оформления практической работы и презентации: 2 балла – работа имеет логичное, последовательное изложение материала. презентация дополняет и иллюстрирует доклад; 1 балл – работа в целом имеет, последовательное изложение материала, однако презентация содержит только тезисы доклада; 0 баллов - просматривается непоследовательность изложения материала, презентация не соответствует содержанию доклада. 3. Качество выступления: 2 балла – студент демонстрирует глубокое знание вопросов темы, грамотно формулирует выводы и предложения, уверенно отвечает на уточняющие вопросы; 1 балл – в процессе выступления студент в целом показывает знание вопросов темы, однако затрудняется при формулировании выводов и предложений, неуверенно отвечает на</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>

	<p>уточняющие вопросы; 0 баллов – студент проявляет неуверенность, демонстрирует слабое знание вопросов темы, не в состоянии сформулировать выводы и предложения. Максимальное количество баллов - 6. Весовой коэффициент - 1.</p>	
Зачет	<p>В процессе зачета происходит оценивание учебной деятельности обучающихся по дисциплине. 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). При проведении зачета студенты в аудитории письменно отвечают на вопросы билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает.</p> <p>Показатели оценивания ответов по каждому из вопросов: 5 баллов – студент обладает твёрдым и полным знанием материала дисциплины, уверенно отвечает на дополнительные вопросы, логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы; 4 балла – студент знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или допускает несущественные неточности; грамотно и по существу излагает материал. 3 балла – студент знает только основной материал дисциплины, не усвоил его деталей, допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности 2 балла – студент не знает значительной части материала дисциплины; допускает грубые ошибки при ответе на дополнительные вопросы; неверно излагает и интерпретирует знания; изложение материала логически не выстроено. Максимальное число баллов - 10.</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>
Бонусное задание	<p>Студент представляет копии документов, подтверждающие победу или участие в конференции. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %.</p>	<p>Зачтено: За выступление с последующей публикацией: на скопус-конференции – 15 %, на Всероссийской конференции (БИП) или за публикацию в журнале ВАК – 12 %. За участие в студенческой научной конференции ЮУрГУ - 3%. За диплом 1-й степени на конференции - +3 %, за диплом 2-й степени на конференции - +2 %, за</p>



		диплом 3-й степени на конференции - +1 %. Не зачтено: не предусмотрено.
--	--	--

### 7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Тестирование	
Выступление с докладом на практических занятиях	
Зачет	
Бонусное задание	

## 8. 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. Прохоров, А. В. Основы защиты информации [Текст] : метод. указания к практ. занятиям / А. В. Прохоров, С. В. Денисов ; Юж.-Урал. гос. ун-т, Озерск. фил., Каф. Информатика ; ЮУрГУ. – Челябинск : Издательский Центр ЮУрГУ, 2012. – 38 с.:ил.

2. Лекции преподавателя

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

1. Прохоров, А. В. Основы защиты информации [Текст] : метод. указания к практ. занятиям / А. В. Прохоров, С. В. Денисов ; Юж.-Урал. гос. ун-т, Озерск. фил., Каф. Информатика ; ЮУрГУ. – Челябинск : Издательский Центр ЮУрГУ, 2012. – 38 с.:ил.

2. Лекции преподавателя

### Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
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	Электронно-	Белоус, А. И. Кибербезопасность объектов топливно-

	литература	библиотечная система издательства Лань	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>

## 9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

## 10. 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+