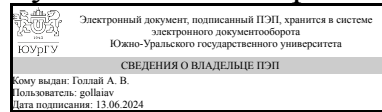


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Руководитель направления



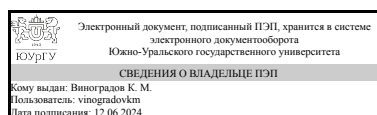
А. В. Голлай

## РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.15 Организационная защита информации  
для направления 09.03.01 Информатика и вычислительная техника  
уровень Бакалавриат  
форма обучения заочная  
кафедра-разработчик Техника, технологии и строительство

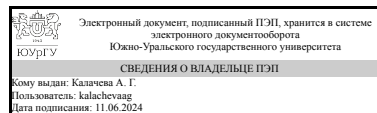
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, утверждённым приказом Минобрнауки от 19.09.2017 № 929

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



К. М. Виноградов

Разработчик программы,  
к.экон.н., доцент



А. Г. Калачева

## 1. Цели и задачи дисциплины

Целью преподавания дисциплины является подготовка специалистов в области управления и организации информационной безопасности, имеющих первичные навыки принятия решения на основе многочисленных нормативно-правовых актов в сфере информационной безопасности, и владеющих общими принципами организации и правового регулирования защиты информации. Задачи дисциплины: - изучение основных нормативных правовых актов международного, федерального и ведомственно-отраслевого уровней, определяющих организационные и правовые аспекты в области информационной безопасности; - изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационного и правового обеспечения информационной безопасности; - ознакомление с процессами планирования в организации защиты информации; - рассмотрение методов и особенностей, применяемых в организации защиты информации в зависимости от характера защищаемой информации; - изучение методов анализа деятельности организаций с целью определения информационно-технологических ресурсов, подлежащих защите.

## Краткое содержание дисциплины

Основные понятия защиты информации. Информация как объект защиты. Методология защиты информации. Криптографические методы защиты информации. Безопасность вычислительных сетей.

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

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает: основные нормативные правовые акты в области обеспечения информационной безопасности. Умеет: применять действующую законодательную базу в области обеспечения информационной безопасности. Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности.
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Знает: структуру документов и нормативные требования к их составлению. Умеет: разрабатывать технические задания на создание подсистем информационной безопасности. Имеет практический опыт: работы с документами.

## 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.16 Метрология, стандартизация и сертификация,	Не предусмотрены

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

Дисциплина	Требования
1.О.13 Компьютерные сети и телекоммуникации	<p>Знает: общие характеристики коммутационного оборудования; принципы планирования и документирования локальных вычислительных сетей., характеристики сетевого оборудования и принципы его установки и подключения; принципы работы CLI сетевого оборудования различных вендоров; характеристики коммутационных кабелей и принципы их прокладки; методы инсталляции сетевого программного обеспечения на сетевое оборудование и персональные компьютеры., принципы установки и конфигурирования коммутационного оборудования. Интерфейс командной строки на коммутационном оборудовании. Методы диагностики сетей и поиска неисправностей. Умеет: планировать сеть на основе требований предъявляемых к сети и технической документации оборудования; планировать обновление сети на основе растущих требований к вычислительной сети., создавать и настраивать локальную сеть согласно техническим требованиям. Подбирать оптимальную конфигурацию сетевого оборудования для сетей различной сложности на основе характеристик сетевого оборудования. Проводить настройку персонального компьютера и сетевого оборудования для работы в локальной сети. Инсталлировать сетевое программное обеспечение на персональный компьютер и сетевое оборудование. , использовать CLI и веб интерфейс для конфигурирования оборудования. Проводить подключение конечных узлов и сетевого оборудования к локальной сети. Обнаруживать неисправность в локальной вычислительной сети. Имеет практический опыт: планирования, обновления и документирования сети малого предприятия., работы с коммутационными шкафами. Работы с инструментами для обжима и заделки кабеля типа "витая пара", обжима и укладки коммутационного кабеля, монтажа локальной сети. Обновления/восстановления/резервного копирования программного обеспечения сетевого оборудования. , построения локальной вычислительной сети второго и третьего уровня. Работы с оборудованием для монтажа коммутационных кабелей. Работы с оборудованием для поиска неисправностей на</p>

	коммутационных линиях.
1.О.16 Метрология, стандартизация и сертификация	Знает: общие положения основных стандартов в области метрологии, стандартизации и сертификации., основы сертификации средств измерения и контроля, структуру и принципы работы измерительных устройств. Умеет: применять методику стандартов по метрологии для обработки результатов измерений в профессиональной деятельности., находить и определять область применения различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества. Собрать измерительную схему. Имеет практический опыт: владеет терминологией в области метрологии, стандартизации и сертификации, навыками обработки результатов измерений., использования различных категорий и видов стандартов, систем стандартов, классификаторов и указателей, документацией продукции, процессов, услуг и систем качества. Навыками использования различных средств измерения.

#### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 18,25 ч. контактной работы с применением дистанционных образовательных технологий

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	12	12	
Лекции (Л)	8	8	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	4	4	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	89,75	89,75	
Подготовка к практическим занятиям	16	16	
Выполнение заданий ЭУК в "Электронном ЮУрГУ"	40	40	
Подготовка к зачету	33,75	33,75	
Консультации и промежуточная аттестация	6,25	6,25	
Вид 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 понятия защиты информации	2	2	0	0
2	Информация как объект защиты. Методология защиты информации	2	2	0	0
3	Криптографические методы защиты информации	4	2	2	0
4	Безопасность вычислительных сетей	4	2	2	0

### 5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие информационной безопасности. Методы обеспечения информационной безопасности в РФ. Реализация государственной политики обеспечения информационной безопасности РФ. Организационная основа системы обеспечения информационной безопасности. Понятие защиты информации в российском законодательстве. Угрозы и уязвимости при защите информации.	2
2	2	Понятие защищаемой информации. Критерии отнесения общедоступной информации к защищаемой. Понятие объекта защиты. Государственная тайна. Служебная тайна. Коммерческая тайна. Профессиональная тайна. Персональные данные. Объекты интеллектуальной собственности. Угрозы защищаемой информации. Виды и методы защиты информации.	2
3	3	Понятие и требования к криптосистемам. Основные алгоритмы шифрования. Симметричные криптосистемы. Ассиметричные криптосистемы. Электронная цифровая подпись.	2
4	4	Классификация угроз, атак в вычислительных сетях. Защитные механизмы обеспечения безопасности вычислительных сетей.	2

### 5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	3	Применение алгоритмов шифрования данных.	2
2	4	Проектирование системы программной аутентификации и авторизации пользователей.	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 к практическим занятиям	Занятие 1: ЭУМЛ №2: Гл. 4; ЭУМЛ №4: Гл. 2. Занятие 2: ЭУМЛ №2: Гл. 8.	9	16
Выполнение заданий ЭУК в "Электронном ЮУрГУ"	<a href="https://edu.susu.ru">https://edu.susu.ru</a>	9	40
Подготовка к зачету	ЭУМЛ №1: Темы 1-5, 7-9, 11; ЭУМЛ №2:	9	33,75

## 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	Учитывается в ПА
1	9	Текущий контроль	Тест №1	0,2	5	Выполнение тестового задания осуществляется на портале «Электронный ЮУрГУ» ( <a href="https://edu.susu.ru">https://edu.susu.ru</a> ). Студенту предоставляется 2 попытки с ограничением по времени для прохождения каждого теста. Метод оценивания – высшая оценка по итогам всех попыток. В случае, если студент набирает менее 60% баллов, по его просьбе преподаватель предоставляет дополнительные попытки.	зачет
2	9	Текущий контроль	Тест №2	0,25	5	Выполнение тестового задания осуществляется на портале «Электронный ЮУрГУ» ( <a href="https://edu.susu.ru">https://edu.susu.ru</a> ). Студенту предоставляется 2 попытки с ограничением по времени для прохождения каждого теста. Метод оценивания – высшая оценка по итогам всех попыток. В случае, если студент набирает менее 60% баллов, по его просьбе преподаватель предоставляет дополнительные попытки.	зачет
3	9	Текущий контроль	Тест №3	0,3	5	Выполнение тестового задания осуществляется на портале «Электронный ЮУрГУ» ( <a href="https://edu.susu.ru">https://edu.susu.ru</a> ). Студенту предоставляется 2 попытки с ограничением по времени для прохождения каждого теста. Метод оценивания – высшая оценка по итогам всех попыток. В случае, если студент набирает менее 60% баллов, по его просьбе преподаватель предоставляет дополнительные попытки.	зачет
4	9	Текущий контроль	Тест №4	0,25	5	Выполнение тестового задания осуществляется на портале «Электронный ЮУрГУ» ( <a href="https://edu.susu.ru">https://edu.susu.ru</a> ). Студенту предоставляется 2 попытки с	зачет

						ограничением по времени для прохождения каждого теста. Метод оценивания – высшая оценка по итогам всех попыток. В случае, если студент набирает менее 60% баллов, по его просьбе преподаватель предоставляет дополнительные попытки.	
5	9	Промежуточная аттестация	Задание промежуточной аттестации	-	10	Промежуточная аттестация проводится на портале «Электронный ЮУрГУ» ( <a href="https://edu.susu.ru">https://edu.susu.ru</a> ). В назначенное по расписанию время студент проходит видео- и аудио-идентификацию и выполняет итоговый тест. Студенту предоставляется 1 попытка с ограничением по времени для прохождения теста. Попытки оцениваются автоматически: максимальный балл за каждый вопрос - 1. Количество вопросов - 10. Метод оценивания — высшая оценка. Мероприятие промежуточной аттестации данной дисциплины не является обязательным мероприятием.	зачет
6	9	Бонус	Бонусное задание (олимпиада)	-	15	Студент представляет копии документов, подтверждающие победу или участие в предметных олимпиадах по темам дисциплины. Максимально возможная величина бонус-рейтинга +15 %.	зачет

## 6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Во время зачета происходит оценивание учебной деятельности обучающихся по дисциплине на основе взвешенной суммы полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и задание промежуточной аттестации.	В соответствии с пп. 2.5, 2.6 Положения

## 6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ					
		1	2	3	4	5	6
ОПК-3	Знает: основные нормативные правовые акты в области обеспечения информационной безопасности.	+					++
ОПК-3	Умеет: применять действующую законодательную базу в области обеспечения информационной безопасности.		+				++
ОПК-3	Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности.				+	+	++
ОПК-4	Знает: структуру документов и нормативные требования к их составлению.		+				++
ОПК-4	Умеет: разрабатывать технические задания на создание подсистем информационной безопасности.				+	+	++
ОПК-4	Имеет практический опыт: работы с документами.	+					++

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. Астахова, Л. В. Теория информационной безопасности и методология защиты информации [Текст] учеб. пособие по специальности 090915 "Безопасность информ. технологий в правоохранит. сфере" и др. специальностям Л. В. Астахова ; Юж.-Урал. гос. ун-т, Каф. Безопасность информ. систем ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 136, [1] с. -  
[https://lib.susu.ru/ftd?base=SUSU\\_METHOD&key=000540003&dtype=F&etype=.pdf](https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000540003&dtype=F&etype=.pdf).

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

1. Астахова, Л. В. Теория информационной безопасности и методология защиты информации [Текст] учеб. пособие по специальности 090915 "Безопасность информ. технологий в правоохранит. сфере" и др. специальностям Л. В. Астахова ; Юж.-Урал. гос. ун-т, Каф. Безопасность информ. систем ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 136, [1] с. -  
[https://lib.susu.ru/ftd?base=SUSU\\_METHOD&key=000540003&dtype=F&etype=.pdf](https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000540003&dtype=F&etype=.pdf).

### Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронный каталог ЮУрГУ	Астахова, Л. В. Теория информационной безопасности и методология защиты информации [Текст] учеб. пособие по специальности 090915 "Безопасность информ. технологий в правоохранит. сфере" и др. специальностям Л. В. Астахова ; Юж.-Урал. гос. ун-т, Каф. Безопасность информ. систем ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 136, [1] с. - <a href="https://lib.susu.ru/ftd?base=SUSU_METHOD&amp;key=000540003&amp;dtype=F&amp;etype=.pdf">https://lib.susu.ru/ftd?base=SUSU_METHOD&amp;key=000540003&amp;dtype=F&amp;etype=.pdf</a>
2	Основная литература	Электронно-библиотечная система	Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — Самара : АСИ СамГТУ, 2014. — 114 с. — ISBN 978-5-7906-0603-3. — Текст : электронный // Лань : электронно-библиотечная система



		издательства Лань	<a href="https://e.lanbook.com/book/73915">https://e.lanbook.com/book/73915</a>
3	Основная литература	Электронно-библиотечная система издательства Лань	Малюк, А. А. Теория защиты информации / А. А. Малюк. — Москва : Горячая линия-Телеком, 2015. — 184 с. — ISBN 978-5-9912-0246-6. — Текст : электронный // Лань : электронно-библиотечная система. <a href="https://e.lanbook.com/book/111077">https://e.lanbook.com/book/111077</a>
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 176 с. — Текст : электронный // Лань : электронно-библиотечная система. <a href="https://e.lanbook.com/book/176563">https://e.lanbook.com/book/176563</a>
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие / В. К. Новиков. — Москва : Горячая линия-Телеком, 2021. — 176 с. — ISBN 978-5-9912-0525-2. — Текст : электронный // Лань : электронно-библиотечная система. <a href="https://e.lanbook.com/book/111084">https://e.lanbook.com/book/111084</a>
6	Дополнительная литература	Электронно-библиотечная система издательства Лань	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандриченко. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-0111-1. — Текст : электронный // Лань : электронно-библиотечная система. <a href="https://e.lanbook.com/book/175506">https://e.lanbook.com/book/175506</a>

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (<https://edu.susu.ru>)(бессрочно)

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
Зачет	118а (2)	Компьютер 15 шт.(Intel(R) Celeron(R) CPU J1800 @ 2.41 GHz, 4,00 ГБ ОЗУ с выходом в Интернет и доступом в портал «Электронный ЮУрГУ»); Компьютер 1 шт. (Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz, 8,00 ГБ ОЗУ); Интерактивная доска IQBoard PS, Проектор EPSON, наушники с микрофоном Logitech, Монитор-15 шт. Microsoft – Windows (бессрочно), Microsoft-Office (бессрочно)
Лекции	118а (2)	Компьютер 15 шт.(Intel(R) Celeron(R) CPU J1800 @ 2.41 GHz, 4,00 ГБ ОЗУ с выходом в Интернет и доступом в портал «Электронный ЮУрГУ»); Компьютер 1 шт. (Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz, 8,00 ГБ ОЗУ); Интерактивная доска IQBoard PS, Проектор EPSON, наушники с микрофоном Logitech, Монитор-15 шт. Microsoft – Windows (бессрочно), Microsoft-Office (бессрочно)
Самостоятельная	118а	Компьютер 15 шт.(Intel(R) Celeron(R) CPU J1800 @ 2.41 GHz, 4,00 ГБ

работа студента	(2)	ОЗУ с выходом в Интернет и доступом в портал «Электронный ЮУрГУ»; Компьютер 1 шт. (Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz, 8,00 ГБ ОЗУ); Интерактивная доска IQBoard PS, Проектор EPSON, наушники с микрофоном Logitech, Монитор-15 шт. Microsoft – Windows (бессрочно), Microsoft-Office (бессрочно)
Практические занятия и семинары	118а (2)	Компьютер 15 шт.(Intel(R) Celeron(R) CPU J1800 @ 2.41 GHz, 4,00 ГБ ОЗУ с выходом в Интернет и доступом в портал «Электронный ЮУрГУ»; Компьютер 1 шт. (Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz, 8,00 ГБ ОЗУ); Интерактивная доска IQBoard PS, Проектор EPSON, наушники с микрофоном Logitech, Монитор-15 шт. Microsoft – Windows (бессрочно), Microsoft-Office (бессрочно)