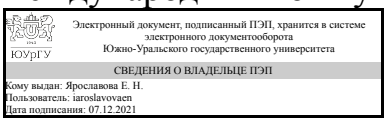
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Институт лингвистики и международных коммуникаций



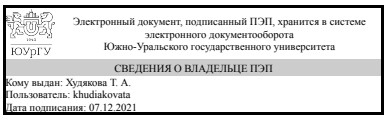
Е. Н. Ярославова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.16 Основы информационной безопасности в профессиональной деятельности
для специальности 45.05.01 Перевод и переводоведение
уровень Специалитет
форма обучения очная
кафедра-разработчик Цифровая экономика и информационные технологии

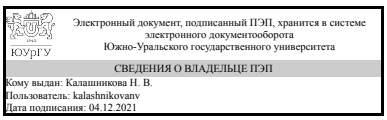
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 45.05.01 Перевод и переводоведение, утверждённым приказом Минобрнауки от 12.08.2020 № 989

Зав.кафедрой разработчика,
д.экон.н., доц.



Т. А. Худякова

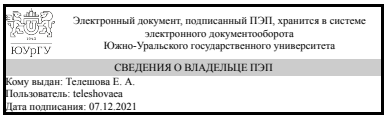
Разработчик программы,
старший преподаватель



Н. В. Калашникова

СОГЛАСОВАНО

Руководитель специальности
к.пед.н.



Е. А. Телешова

Челябинск

1. Цели и задачи дисциплины

Цель изучения и преподавания дисциплины «Основы информационной безопасности в профессиональной деятельности» определена ФГОС – подготовка специалистов, которые понимают сущность и значение информации в развитии современного информационного общества, сознают опасности и угрозы, возникающие в этом процессе, знают методы защиты информации и соблюдают основные требования информационной безопасности. Задачи курса – овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности, освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения.

Краткое содержание дисциплины

В процессе освоения дисциплины изучаются следующие разделы. • Информационная безопасность как составляющая общественной безопасности. Основные понятия информационной безопасности и защиты информации. • Виды и особенности угроз информационной безопасности. Критерии классификации угроз. Основные составляющие обеспечения информационной безопасности. • Законодательный уровень информационной безопасности. Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа. • Стандарты и спецификации в области информационной безопасности. • Административный уровень информационной безопасности. • Процедурный уровень информационной безопасности. • Защищенный документооборот. • Программно-технический уровень информационной безопасности. Инженерно-техническая защита информации. • Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	Знает: концепцию информационной безопасности, конституционные и законодательные основы ее реализации; задачи информационной безопасности; направления и методы обеспечения безопасности информационных ресурсов; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности. Умеет: проводить анализ степени защищенности информации; повысить защиты с учетом развития математического и программного обеспечения вычислительных систем. Имеет практический опыт: обеспечения защиты информации и безопасного использования программных средств в вычислительных

	системах; навыками использования средств и систем защиты информации.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.08 Политология, 1.О.13 Концепции современного естествознания, 1.О.09 Социология, 1.О.36 Безопасность жизнедеятельности, 1.О.14 Экология	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.08 Политология	Знает: основы обеспечения развития общества в том числе при угрозе ЧС и военных конфликтов., основные теории, понятия и модели политологии; основы политической жизни стран изучаемого языка; место и роль стран изучаемого языка в региональных и глобальных процессах. Умеет: создавать и поддерживать в профессиональной деятельности безопасные условия жизнедеятельности; обеспечивать развитие общества при угрозе возникновения чрезвычайных ситуаций и военных конфликтов. , применять понятийно-категориальный аппарат, основные законы политологии в процессе осуществления межъязыкового и межкультурного взаимодействия; корректно использовать в своей деятельности профессиональную этику. Имеет практический опыт: использования теоретических знаний на практике; создания и поддерживания безопасных условий жизнедеятельности., владения навыками целостного подхода к анализу проблем политической сферы общества.
1.О.14 Экология	Знает: основные методы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий; условия жизнедеятельности, необходимые для сохранения природной среды; теоретические основы безопасности жизнедеятельности при ЧС; возможные последствия аварий, катастроф, стихийных бедствий и способы применения современных средств поражения; правовые, нормативно-технические и организационные основы безопасности жизнедеятельности. Умеет: поддерживать в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды; идентифицировать

	основные опасности среды обитания человека, оценивать риск их реализации; принимать решения по целесообразным действиям в ЧС; распознавать жизненные нарушения при неотложных состояниях и травмах. Имеет практический опыт: владения приемами и способами использования индивидуальных средств защиты в ЧС; основными методами защиты производственного персонала и населения при возникновении ЧС; приемами оказания первой помощи пострадавшим в ЧС и экстремальных ситуациях.
1.О.09 Социология	Знает: понятийный аппарат социологии; основные социологические концепции стран Запада и России, специфику социокультурного развития страны., основы обеспечения развития общества в том числе при угрозе ЧС и военных конфликтов. Умеет: давать объективную оценку различным социальным явлениям и процессам, происходящим в обществе; осуществлять межкультурное взаимодействие на основе знаний в области социальной жизни стран изучаемого языка., поддерживать в профессиональной деятельности безопасные условия жизнедеятельности; обеспечивать развитие общества при угрозе возникновения чрезвычайных ситуаций и военных конфликтов. Имеет практический опыт: анализа социальных явлений и процессов для осуществления межкультурного взаимодействия., использования теоретических знаний на практике; создания и поддерживания безопасных условий жизнедеятельности общества.
1.О.13 Концепции современного естествознания	Знает: принципы научного познания действительности; современную научную картину мира, место и роль человека в ней; основы естественно-научных дисциплин в едином комплексе наук; глобальные проблемы человечества. Умеет: отличать научно обоснованные представления от псевдонаучных; глобально мыслить; готовить рефераты и презентации по глобальным проблемам человечества; вскрывать универсальность законов самоорганизации для всех уровней материального мира; применять полученные знания для изучения других предметов, расширения кругозора, обеспечения безопасных условий жизнедеятельности. Имеет практический опыт: решения задач и проблем в области сохранения окружающей среды на основе концептуального подхода; ведения дискуссии по фундаментальным и мировоззренческим темам; противостояния псевдонаучной аргументации.
1.О.36 Безопасность жизнедеятельности	Знает: основы обеспечения развития общества в том числе при угрозе ЧС и военных конфликтов;

	основные методы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий Умеет: поддерживать в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды; обеспечивать развитие общества при угрозе возникновения чрезвычайных ситуаций и военных конфликтов. Имеет практический опыт: использования теоретических знаний на практике; создания и поддерживания безопасных условий жизнедеятельности.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	35,75	35,75
с применением дистанционных образовательных технологий	0	
Подготовка к зачету	16	16
Подготовка к практическим занятиям	19,75	19.75
Консультации и промежуточная аттестация	4,25	4,25
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	Информационная безопасность как составляющая общественной безопасности. Основные понятия информационной безопасности и защиты информации.	4	2	2	0
2	Виды и особенности угроз информационной безопасности. Критерии классификации угроз. Основные составляющие обеспечения информационной безопасности.	4	2	2	0
3	Законодательный уровень информационной безопасности. Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа.	4	2	2	0

4	Стандарты и спецификации в области информационной безопасности.	4	2	2	0
5	Административный уровень информационной безопасности. Управление рисками.	4	2	2	0
6	Процедурный уровень информационной безопасности. Защищенный документооборот.	4	2	2	0
7	Программно-технический уровень информационной безопасности. Инженерно-техническая защита информации.	4	2	2	0
8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.	4	2	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Информационная безопасность как составляющая общественной безопасности: понятие безопасности, концепция информационной безопасности России, международные доктрины в области информационной безопасности. Информационная безопасность как институт информационного права. Основные понятия информационной безопасности и защиты информации, соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации.	2
2	2	Виды и особенности угроз информационной безопасности: основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. Риски угроз информационным ресурсам. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений. Основные составляющие обеспечения информационной безопасности. Информационная безопасность и компьютеризация информационной среды.	2
3	3	Законодательный уровень информационной безопасности. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования. Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа: понятие тайны, секрета, конфиденциальности. Субъекты и объекты информационных правоотношений в области государственной тайны, коммерческой тайны, производственной тайны, служебной тайна, профессиональной тайн. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Конфиденциальная информация и ее виды. Персональные данные. Конфиденциальность информации в вычислительных системах и сетях.	2
4	4	Стандарты и спецификации в области информационной безопасности.	2
5	5	Административный уровень информационной безопасности. Управление рисками. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Принципы учета конфиденциальных документов. Технология обработки и хранения конфиденциальных документов.	2
6	6	Процедурный уровень информационной безопасности. Понятие, цели и задачи системы защиты конфиденциальной информации. Разграничение	2

		уровня конфиденциальности сведений. Регламентация технологии защиты информации от потенциальных и реальных угроз. Доступ персонала к конфиденциальным сведениям, документам и базам данных. Защищенный документооборот: понятие и задачи защищённого документооборота; технологические системы защиты и обработки конфиденциальных документов; принципы учета конфиденциальных документов; технология обработки конфиденциальных документов. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.	
7	7	Программно-технический уровень информационной безопасности. Инженерно-техническая защита информации. Классификация и характеристика групп технических средств охраны. Охранные системы. Технические средства идентификации. Аппаратные средства защиты.	2
8	8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.Программно-технические методы обеспечения информационной безопасности: идентификация и аутентификация, управление доступом; протоколирование и аудит; шифрование, контроль целостности; межсетевые экраны как средство защиты от несанкционированного доступа, анализ защищенности; обеспечение высокой доступности.Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макровирусы, скрипт вирусы, вирусы-мистификации. Профилактика вирусно-го заражения. Антивирусные программы. Методика применения антивирусных программ. Криптографические средства защиты. Криптографическое пре-образование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Информационная безопасность как составляющая общественной безопасности. Основные понятия информационной безопасности и защиты информации.	2
2	2	Виды и особенности угроз информационной безопасности. Критерии классификации угроз. Основные составляющие обеспечения информационной безопасности.	2
3	3	Законодательный уровень информационной безопасности. Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения.	2
4	4	Стандарты и спецификации в области информационной безопасности.	2
5	5	Административный уровень информационной безопасности. Управление рисками.	2
6	6	Процедурный уровень информационной безопасности. Защищенный документооборот: понятие и задачи защищённого документооборота; технологические системы защиты и обработки конфиденциальных	2

		документов; принципы учета конфиденциальных документов; технология обработки конфиденциальных документов.	
7	7	Программно-технический уровень информационной безопасности. Инженерно-техническая защита информации.	2
8	8	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.	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 зачету	Основы информационной безопасности. https://intuit.ru/studies/courses/10/10/info	8	16
Подготовка к практическим занятиям	Основы информационной безопасности. https://intuit.ru/studies/courses/10/10/info	8	19,75

6. Текущий контроль успеваемости, промежуточная аттестация

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	8	Текущий контроль	Практические задания по разделам 1-6	1	42	Защита практической работы осуществляется индивидуально. Студентом предоставляется выполненное задание на компьютере. Оценивается качество оформления, правильность выполнения задания. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: - задание выполнено в полном объеме, качественно оформлено - 7 баллов; - задание выполнено не полностью либо оформлено не качественно - 5 баллов; -задание выполнено поверхностно - 2	зачет

						балла; - задание не выполнено - 0 баллов. Максимальное количество баллов – 7 за задание (всего 6 заданий). Весовой коэффициент мероприятия – 1.	
2	8	Текущий контроль	Практические задания по разделам 7-8	1	18	Защита практической работы осуществляется индивидуально. Студентом предоставляется выполненное задание на компьютере. Оценивается качество оформления, правильность выполнения задания. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: - задание выполнено в полном объеме, качественно оформлено - 9 баллов; - задание выполнено не полностью либо оформлено не качественно - 5 баллов; -задание выполнено поверхностно - 2 балла; - задание не выполнено - 0 баллов. Максимальное количество баллов – 9 за задание (всего 2 задания). Весовой коэффициент мероприятия – 1.	зачет
3	8	Проме-жуточная аттестация	Зачет	-	40	Проводится в форме тестирования. Количество вопросов, формируемых компьютером самостоятельно - 40 Время, отводимое на тестирование 40 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценивания: правильный ответ на вопрос теста соответствует 1 баллу. Максимальное количество баллов 40. Весовой коэффициент мероприятия 1	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Проводится в форме тестирования. Количество вопросов, формируемых компьютером самостоятельно - 40 Время, отводимое на тестирование 40 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценивания: правильный ответ на вопрос	В соответствии с пп. 2.5, 2.6 Положения

	теста соответствует 1 баллу. Максимальное количество баллов 40. Весовой коэффициент мероприятия 1	

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ		
		1	2	3
УК-8	Знает: концепцию информационной безопасности, конституционные и законодательные основы ее реализации; задачи информационной безопасности; направления и методы обеспечения безопасности информационных ресурсов; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности.	+	+	+
УК-8	Умеет: проводить анализ степени защищенности информации; повысить защиты с учетом развития математического и программного обеспечения вычислительных систем.	+	+	+
УК-8	Имеет практический опыт: обеспечения защиты информации и безопасного использования программных средств в вычислительных системах; навыками использования средств и систем защиты информации.	+	+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Степанов, Е. А. Информационная безопасность и защита информации Учеб. пособие для вузов по специальности "Документоведение и документацион. обеспечение упр." Е. А. Степанов, И. К. Корнеев. - М.: ИНФРА-М, 2001. - 301,[1] с. ил.
2. Мельников, В. П. Информационная безопасность Учеб. пособие для сред. проф. образования В. П. Мельников, С. А. Клейменов, А. М. Петраков; Под ред. С. А. Клейменова. - М.: Академия, 2005. - 331 с.

б) дополнительная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации [Текст] учеб. пособие по направлению "Приклад. информатика" Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М.: РИОР : ИНФРА-М, 2018. - 334, [1] с. ил.
2. Галицкий, А. В. Защита информации в сети - анализ технологий и синтез решений А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. - М.: ДМК-Пресс, 2004. - 613 с. ил.
3. Завгородний, В. И. Комплексная защита информации в компьютерных системах Учеб. пособие для вузов В. И. Завгородний. - М.: Логос, 2001. - 262, [1] с.
4. Мельников, В. П. Информационная безопасность и защита информации [Текст] учеб. пособие В. П. Мельников и др.; под ред. С. А. Клейменова. - 4-е изд., стер. - М.: Академия, 2009. - 330, [1] с.

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

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Суховилов Б. М. Защита информации в корпоративных информационных системах: учеб. пособие к практ. работам по направлению "Приклад. информатика". Челябинск, 2013.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Суховилов Б. М. Защита информации в корпоративных информационных системах: учеб. пособие к практ. работам по направлению "Приклад. информатика". Челябинск, 2013.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Методические пособия для самостоятельной работы студента	Электронный каталог ЮУрГУ	Суховилов Б. М. Защита информации в корпоративных информационн системах: учеб. пособие к практ. работам по направлению "Приклад. информатика". Челябинск, 2013. https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000513410&dtype=F

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	204 (3г)	Компьютер, проектор, ОС Windows, доступ к интернет.
Практические занятия и семинары	114-2 (2)	Компьютерный класс, ОС Windows, доступ к интернет.
Контроль самостоятельной работы	114-2 (2)	Компьютерный класс, ОС Windows, доступ к интернет.