УТВЕРЖДЕНО:
Ученым советом Института сервисных технологий ФГБОУ ВО «РГУТИС»
Протокол № 7 от «10» февраля 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.В.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена

по специальности: ***09.02.07 Информационные системы и программирование***
Квалификация: ***специалист по информационным системам***

год начала подготовки: 2022

Разработчики:

должность	ученая степень и звание, ФИО
преподаватель	***Ашырглыжов Е.Х.***

Рабочая программа согласована и одобрена руководителем ППССЗ:

должность	ученая степень и звание, ФИО
преподаватель	***к.м.н. Алабина С.А.***

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.11 Информационная безопасность

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.11 «Компьютерные сети» является обязательной частью общепрофессионального цикла примерной основной образовательной программы в соответствии с ФГОС по специальности 09.02.07 Информационные системы и программирование.

Особое значение дисциплина имеет при формировании и развитии ОК 01, ОК 09.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК, ЛР	Умения	Знания
ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10 ЛР 03 ЛР 10 ЛР 19 ЛР 20 ЛР 21	- применять методы и системы защиты информации; - обеспечивать защиту и сохранность данных в сети, - своевременно реагировать на вирусные угрозы и кибератаки - принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации; - администрировать подсистемы информационной безопасности различных объектов информатизации;	- сущность, цели и принципы информационной безопасности, законодательные основы ее реализации; - информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности; - направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты; - методику защиты информации в деятельности организации - функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины	88
в т.ч. в форме практической подготовки	0
в т. ч.:	
теоретическое обучение	34
лабораторные работы *(если предусмотрено)*	0
практические занятия *(если предусмотрено)*	36
курсовая работа (проект) *(если предусмотрено для специальностей*)	0
консультации	2
Самостоятельная работа	4
Промежуточная аттестация (экзамен)	12

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, Практические работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Тема 1. Концепции и аспекты обеспечения информационной безопасности	**Лекционные занятия:**		
	1. Понятия экономической и информационной безопасности. 2. Ключевые вопросы информационной безопасности	**6**	**2**
Тема 2. Виды угроз информационной безопасности	**Лекционные занятия:**		
	3. Виды угроз информационной безопасности 4. Основные виды защищаемой информации	**6**	**2**
	Практическое занятие 1		
	Основы законодательства в области обеспечения информационной безопасности	8	
	Разработка метода и модели системы защиты информации.		
	Алгоритм проведения анализа и оценки угроз.		
Тема 3. Построения системы информационной безопасности	**Лекционные занятия:**	**6**	
	5. Основные аспекты построения системы информационной безопасности 6. Анализ и управление рисками при реализации информационной безопасности		**2**
	Практическое занятие 2	6	
	Адаптивная модель СЗИ на базе нейронных сетей. Схема работы генетического алгоритма		

Тема 4. Защита информации в информационных системах и компьютерных сетях	**Лекционные занятия:**	**6**	**2**
	7. Защита информации в информационных системах и компьютерных сетях.		
	8. Методология анализа защищенности информационной системы.		
	Практическое занятие 3 Трёхуровневая модель параметров оценки защищенности ИС. Модели системы защиты.	6	
Тема 5. Обеспечение безопасности ИС	**Лекционные занятия:**	**6**	**2**
	9. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. 10. Технологии криптографической защиты информации. Современные средства биометрической идентификации.		
	Практическое занятие 4 Защита информации в распределенной ИС. Шифрование и дешифрование данных. Таблица Вижинера	8	
Тема 6. Обеспечение интегральной безопасности ИС	**Лекционные занятия:**	**4**	**2**
	11. Обеспечение интегральной безопасности информационных систем и сетей 12. Технологии криптографической защиты информации.		
	Практическое занятие 5 Распределенная информационная система. Технологии токенов Компоновка VPN на основе международных стандартов и протоколов.	8	
	Самостоятельная работа 5 Систематическая проработка конспектов занятий, учебной и специальной технической литературы по темам:	4	

	Принципы организации разноуровневого доступа в автоматизированных информационных системах. Понятие несанкционированного доступа и защита от него. Управление доступом в информационных системах. Основные понятия: клиент, право и объект доступа, группы, роли, политика безопасности. Дискреционная модель доступа. Преимущества и недостатки. Мандатная модель доступа. Преимущества и недостатки.		
Консультации		**2**	
Промежуточная аттестация (экзамен в 6 семестре)		**12**	
Всего		**88**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализация программы дисциплины должны быть предусмотрены следующие специальные помещения: **Лаборатория «Организации и принципов построения информационных систем»:**
, оснащенные в соответствии с п. 6.1.2.1. Примерной программы по специальности:
–Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО: Eclipse IDE for Java EE Developers, .NETFrameworkJDK 8, Microsoft SQL Server Express Edition,
Microsoft Visio Professional, Microsoft Visual Studio,
MySQL Installer for Windows, Net Beans, SQL Server Management Studio,
Microsoft SQL Server Java Connector, Android Studio, IntelliJIDEA.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1189328

2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1082470

Дополнительные источники:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1189327

2. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И. — Москва : КноРус, 2021. — 267 с.— URL: https://book.ru/book/939292

Интернет – ресурсы:

1. Научно-технический и научно-производственный журнал «Информационные технологии» http://novtex.ru/IT/index.htm
2. Журнал «Информационное общество» http://www.infosoc.iis.ru/
3. Журнал «Бизнес-информатика» https://bijournal.hse.ru/
4. Журнал «Информационные системы и технологии» http://oreluniver.ru/science/journal/isit
5. Журнал «Электронные информационные системы». Режим доступа: https://elins-journal.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
У1 применять методы и системы защиты информации;	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
У2 обеспечивать защиту и сохранность данных в сети,	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
У3 своевременно реагировать на вирусные угрозы и кибератаки	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
У4 принимать участие в эксплуатации подсистем управления информационной	Для текущего контроля: Оценка выполнения практических работ,

безопасностью различных объектов информатизации;	оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
У5 администрировать подсистемы информационной безопасности различных объектов информатизации;	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
З1 сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
З2 информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
З3 направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
З4 методику защиты информации в деятельности организации	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
З5 функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов.	Для текущего контроля: Оценка выполнения практических работ, оценка выполнения самостоятельных работ, устный опрос. Для промежуточной аттестации: экзамен
ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение	

окружающих.	
ЛР 10 Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.	
ЛР 19 Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение	
ЛР 20 Способный в цифровой среде проводить оценку информации, ее достоверность, строя логические умозаключения на основе поступающей информации	
ЛР 21 Предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве	