МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ
«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ РАДИОЭЛЕКТРОНИКИ, ИНФОРМАЦИОННЫХ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»
(ГБПОУ РО «РКРИПТ»)

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность:
09.02.07 Информационные системы и программирование

Квалификация выпускника:
программист

Форма обучения: очная

Ростов-на-Дону
2023

СОГЛАСОВАНО
Начальник методического отдела
_____ Н.В. Вострякова
«26» апреля 2023 г.

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
_____ С.А. Будасова
«26» апреля 2023 г.

ОДОБРЕНО
Цикловой комиссией
вычислительной техники и
компьютерных сетей
Пр. № 8 от «26» апреля 2023 г.

Председатель ЦК
_____ Е.И. Кучкова

Рабочая программа учебной дисциплины ОП.13 Информационная безопасность разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденным Приказом Министерства образования и науки Российской Федерации от «09» декабря 2016 г. №1547 (зарегистрирован Министерством юстиции Российской Федерации «26» декабря 2016 г., регистрационный №44936), с учетом требований профессионального стандарта 06.001 Программист, утвержденного приказом Министерства труда и социальной защиты РФ от «20» июля 2022 г. № 424н.

Разработчик(и):
Шаулова Е.В. – преподаватель ГБПОУ РО «РКРИПТ»

Рецензенты:
Горбачук М.А. – преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ»
Скрынников В.Д. – генеральный директор ООО «ОП»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Учебная дисциплина «ОП.13 Информационная безопасность» является вариативной частью общепрофессионального цикла программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.07 Информационные системы и программирование.

Учебная дисциплина «ОП.13 Информационная безопасность» обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС СПО по специальности 09.02.07 Информационные системы и программирование. Особое значение дисциплина имеет при формировании и развитии общих, профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.

ПК 4.3. Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика.

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.

ЛР 20. Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целей в цифровой среде.

ЛР 26 Развивающий творческие способности, способный креативно мыслить.

ЛР29. Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.

ЛР30.Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм.

ЛР 31. Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

ЛР32.Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению.

ЛР33.Принимающий цели и задачи научно-технического, экономического, информационного развития России, готовый работать на их достижение.

ЛР34. Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

ЛР 35. Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации.

ЛР 37. Осуществляющий поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	**Умения**	**Знания**
ОК 01, ОК 02, ОК 04, ОК 05, ОК 09; ПК 4.1., ПК 4.3., ПК 4.4., ПК 7.3., ПК 7.5; ЛР 20, 26, 29, 30-35, 37	- применять правовые, организационные, технические и программные средства защиты информации; - использовать стандартные инструменты криптографической и антивирусной защиты, предоставляемые различными файловыми системами и специальными программами; - производить настройку операционной системы специальными средствами настройки безопасности при работе в компьютерных сетях.	- источники возникновения информационных угроз; - уровни защиты информации от несанкционированного доступа; - методы криптографической и антивирусной защиты информации; - состав и методы организационно-правовой защиты информации.

1.3 Практическая подготовка при реализации учебных дисциплин

Практическая подготовка - форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей образовательной программы

№ п/п	Раздел	№, название темы	Вид учебного занятия/ учебной деятельности название	Объем часов по учебной дисциплине	
				по разделу/ теме	в том числе на практическую подготовку по указанному занятию
1	Раздел 1. Основные направления государственной политики в сфере информационной безопасности	Тема 1.1 Основные понятия. Законодательство РФ в области информационной безопасности	Лекционное занятие/Практическое занятие № 1. Изучение правовых документов государственной политики в сфере информационной безопасности	10/6	6
2	Раздел 1. Основные направления государственной политики в сфере информационной безопасности	Тема 1.2 Уровни защиты информации	Лекционное занятие	10/2	2
3	Раздел 1. Основные направления государственной политики в сфере информационной безопасности	Тема 1.3 Классификация основных угроз безопасности информации	Лекционное занятие	10/2	2
4	Раздел 2. Основные принципы защиты информации	Тема 2.1 Основные правила защиты информации на	Лекционное занятие/Практическое занятие № 2. Методы блокирования доступа к ПК	20/4	4

	на персональном компьютере	ПК. Методы блокирования доступа к ПК			
5	Раздел 2. Основные принципы защиты информации на персональном компьютере	Тема 2.2 Резервное копирование и восстановление данных.	Лекционное занятие/Практическое занятие № 3. Архивация и резервное копирование данных.	20/4	4
6	Раздел 2. Основные принципы защиты информации на персональном компьютере	Тема 2.3 Современная криптография. Основные криптографические алгоритмы	Лекционное занятие/Практическое занятие № 4. Шифрование, дешифрование информации с применением криптографических алгоритмов.	20/6	6
7	Раздел 2. Основные принципы защиты информации на персональном компьютере	Тема 2.4 Основные методы защиты информации от компьютерных вирусов	Лекционное занятие/Практическое занятие № 5. Установка и изучение возможностей антивирусных программ.	20/6	6
8	Раздел 3. Основы информационной безопасности при работе в компьютерных сетях	Тема 3.1 Основные угрозы при работе в компьютерных сетях	Лекционное занятие/Практическое занятие № 6. Настройки безопасности компьютеров в сети Интернет	18/4	4
9	Раздел 3. Основы информационной безопасности при работе в компьютерных сетях	Тема 3.2 Основные методы защиты информации в компьютерных сетях	Лекционное занятие/Практическое занятие № 7. Настройка параметров безопасности. Установка параметров шифрования	18/6	6
10	Раздел 3. Основы информационной безопасности при работе в компьютерных сетях	Тема 3.3 Настройка защиты информационнй системы в компьютерной сети	Лекционное занятие/Практическое занятие № 8. Создание схем подключения межсетевых экранов	18/4	4
11	Раздел 3. Основы информационной безопасности	Тема 3.4 Основные принципы обеспечения безопасности	Лекционное занятие/Практическое занятие № 9. Настройка защищенного беспроводного	18/4	4

	при работе в компьютерных сетях	информации в беспроводных сетях.	соединения		
12	Экзамен			6/6	6
13	Итого			54 / 48	48

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем учебной дисциплины	**54**
в том числе в форме практической подготовки	**54**
Самостоятельная учебная работа	
Суммарная учебная нагрузка во взаимодействии с преподавателем	**48**
в том числе:	
теоретическое обучение	30
практические занятия	18
лабораторные занятия	**-**
консультации по темам	**-**
Промежуточная аттестация – экзамен (Э)	**6**
консультация	-

2.2. Тематический план и содержание профессионального модуля (ПМ)

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа студентов		Объем часов по учебной дисциплине		Коды компетенций и личностных результатов, формированию которых способствует элемент программы (ПК, ОК, ЛР)
			по разделу, теме	в том числе на практическую подготовку по указанному занятию	
Раздел 1. Основные направления государственной политики в сфере информационной безопасности			**10**	**10**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09; ПК 4.1., ПК 4.3., ПК 4.4., ПК 7.3., ПК 7.5; ЛР 20, 26, 29, 30-35, 37
Тема 1.1 Основные понятия. Законодательство РФ в области информационной безопасности.	**Содержание**		4	4	
	1	Основные документы государственной политики в сфере информационной безопасности.			
	2	Основные стандарты в области информационной безопасности.			
	В том числе, практических занятий		2	2	
	№ 1	Изучение правовых документов государственной политики в сфере информационной безопасности.			
Тема 1.2 Уровни защиты	**Содержание**		2	2	
	1	Правовой, административный, процедурный, организационный уровни защиты информации.			

информации					
	2	Основные функции на каждом уровне.			
	3	Принципы построения политики безопасности.			
Тема 1.3 Классификация основных угроз безопасности информации	**Содержание**		2	2	
	1	Разделение угроз информационной безопасности по категориям. Внутренние и внешние угрозы. Преднамеренные и непреднамеренные угрозы.			
	2	Активные и пассивные угрозы. Угрозы природного и техногенного характера.			
	3	Основные методы предотвращения угроз			
Раздел 2. Основные принципы защиты информации на персональном компьютере			**20**	**20**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09; ПК 4.1., ПК 4.3., ПК 4.4., ПК 7.3., ПК 7.5; ЛР 20, 26, 29, 30-35, 37
Тема 2.1 Основные правила защиты информации на ПК. Методы блокирования доступа к ПК	**Содержание**		2	2	
	1	Основные мероприятия по защите информации на ПК.			
	2	Аутентификация и авторизация. Виды аутентификации			
	В том числе, практических занятий		2	2	
	№ 2	Методы блокирования доступа к ПК			
Тема 2.2 Резервное копирование и восстановление данных.	**Содержание**		2	2	
	1	Причины аварийных ситуаций.			
	2	Резервное копирование и восстановление данных. Создание точек отката системы.			
	В том числе, практических занятий		2	2	
	№ 3	Архивация и резервное копирование данных.			
Тема 2.3 Современная криптография.	**Содержание**		4	4	
	1	Криптографические протоколы, алгоритмы и системы.			
	2	Асимметричные алгоритмы. Принципы организации			

Основные криптографические алгоритмы.		ЭЦП.			
	3	Реализация защиты информации на ПК и при передаче информации с помощью криптосистем PGP и PKI.			
	В том числе, практических занятий		2	2	
	№ 4	Шифрование, дешифрование информации с применением криптографических алгоритмов			
Тема 2.4 Основные методы защиты информации от компьютерных вирусов	**Содержание**		4	4	
	1	История возникновения компьютерных вирусов.			
	2	Пути проникновения компьютерных вирусов в систему.			
	3	Методы классификации компьютерных вирусов. Анализ программной структуры компьютерных вирусов.			
	4	Основные методы защиты информации от компьютерных вирусов.			
	5	Основные антивирусные программы. Методы обнаружения вирусов.			
	В том числе, практических занятий		2	2	
	№ 5	Установка и изучение возможностей антивирусных программ			
Раздел 3. Основы информационной безопасности при работе в компьютерных сетях			**18**	**18**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09; ПК 4.1., ПК 4.3., ПК 4.4., ПК 7.3., ПК 7.5; ЛР 20, 26, 29, 30-35, 37
Тема 3.1 Основные угрозы при работе в компьютерных сетях	**Содержание**		2	2	
	1	Классификация удаленных угроз и их характеристика			
	2	Типовые удаленные угрозы			
	В том числе, практических занятий		2	2	
	№ 6	Настройки безопасности компьютеров в сети Интернет.			

Тема 3.2 Основные методы защиты информации в компьютерных сетях	**Содержание**		4	4	
	1	Безопасность протоколов. Настройки параметров безопасности. Протоколы шифрования. Выбор уровня шифрования. Виртуальные частные сети.			
	В том числе, практических занятий		2	2	
	№ 7	Настройка параметров безопасности. Установка параметров шифрования			
Тема 3.3 Настройка защиты информационной системы в компьютерной сети	**Содержание**		2	2	
	1	Принципы построения системы защиты информации. Основные средства защиты современных корпоративных систем и их инструменты.			
	2	Комплексный подход к организации системы защиты информационных систем.			
	3	Межсетевые экраны. Типы и схемы подключения			
	В том числе, практических занятий		2	2	
	№ 8	Создание схем подключения межсетевых экранов			
Тема 3.4 Основные принципы обеспечения безопасности информации в беспроводных сетях	**Содержание**		2	2	
	1	Угрозы при работе в беспроводных сетях. Стандарты из семейства 802.11x. Управление подключениями в точке беспроводного доступа.			
	2	Дополнительная защита в беспроводных сетях. Достоинства и недостатки удаленного доступа			
	В том числе, практических занятий		2	2	
	№ 9	Настройка защищенного беспроводного соединения			
Консультация			**-**	**-**	
Промежуточная аттестация- экзамен (Э)			**6**	**6**	
Всего:			**54**	**54**	

2.3. Планирование учебных занятий с использованием активных и интерактивных форм и методов обучения

№ п/п	Тема учебного занятия	Активные и интерактивные формы и методы обучения
1	**Тема 1.2 Уровни защиты информации**	Мини-лекция
2	**Тема 1.3 Классификация основных угроз безопасности информации**	Презентации
3	**Тема 2.1 Методы блокирования доступа к ПК**	Презентации
4	**Тема 2.3 Современная криптография. Основные криптографические алгоритмы**	Презентации
5.	**Тема 3.1 Основные угрозы при работе в компьютерных сетях**	Кейс-технологии - решений ситуационных задач

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Реализация программы дисциплины требует наличия учебного кабинета (лаборатории) Информатики**.**

Оборудование учебного кабинета (лаборатории):

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением;
- мультимедиапроектор.

Лицензионное программное обеспечение.

- ОС Windows;
- Microsoft Word;
- Microsoft Excel;
- Microsoft Access;
- Microsoft Visio.

При реализации программы или её части с применением электронного обучения и дистанционных образовательных технологий проведение учебных занятий, выполнение практических работ предусматривает использование учебно-методических материалов в электронном виде, а также наличие у преподавателя и обучающихся:

- персонального компьютера с выходом в интернет;
- Веб-камеры;
- электронной почты;
- программного обеспечения: Cisco Webex, Skype, Zoom и др.

3.2. Информационное обеспечение реализации программы

3.2.1. Печатные издания

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебник для СПО. - М.: Форум, 2019

3.2.2. Электронные издания (электронные ресурсы)

1. www.intuit.ru
2. www.citforum.ru/nets/tcp/tcpspec.shtm
3. Ищейнов В.Я. Основные положения информационной безопасности:

Учебное пособие для СПО / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, ЭБС Знаниум (2018)

4. Партыка Т.Л. Информационная безопасность: Учебное пособие для СПО и вузов / Т.Л. Партыка, И.И. Попов. - М.: Форум, ЭБС Знаниум (2018)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
студент должен знать: - источники возникновения информационных угроз; -уровни защиты информации от несанкционированного доступа; -методы криптографической и антивирусной защиты информации; -состав и методы организационно-правовой защиты информации.	Оценка *«отлично»* выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач; оценка *«хорошо»* выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения; оценка *«удовлетворительно»* выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач; оценка *«неудовлетворительно»* выставляется обучающемуся, который не знает значительной	Тестирование (компьютерное тестирование) на знание терминологии по темам дисциплины; Письменные и устные формы опроса; Оценка выполнения реферативных работ; Наблюдение за выполнением практического задания (деятельностью студента); Оценка выполнения практических заданий; Оценка решений ситуационных задач; Экзамен

	части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.	
студент должен уметь: - применять правовые, организационные, технические и программные средства защиты информации; - использовать стандартные инструменты криптографической и антивирусной защиты, предоставляемые различными файловыми системами и специальными программами; - производить настройку операционной системы специальными средствами настройки безопасности при работе в компьютерных сетях.	Проверка правильности расчетов и осуществления необходимых действий 85 - 100% правильных расчетов и действий – «отлично» 69-84% правильных расчетов и действий – «хорошо» 51-68% правильных расчетов и действий – «удовлетворительно» 50% и менее – «неудовлетворительно»	Тестирование (компьютерное тестирование) на знание терминологии по темам дисциплины; Письменные и устные формы опроса; Оценка выполнения реферативных работ; Наблюдение за выполнением практического задания (деятельностью студента); Оценка выполнения практических заданий; Оценка решений ситуационных задач; Экзамен
личностные результаты: ЛР 20. Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целей в цифровой среде. ЛР 26 Развивающий творческие способности, способный креативно мыслить. ЛР 29. Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.	- демонстрация интереса к будущей профессии; - оценка собственного продвижения, личностного развития; - положительная динамика в организации собственной учебной деятельности по результатам самооценки, самоанализа и коррекции ее результатов; - ответственность за результат учебной деятельности и подготовки к профессиональной деятельности; - участие в исследовательской и проектной работе; - участие в конкурсах	Анкетирование и тестирование Оценка выполнения эссе «Моя будущая профессия» Участие в конкурсах профессионального мастерства, технического творчества, чемпионатах «WorldSkills» Характеристики с мест прохождения практик Наблюдение, анализ соблюдения норм и правил поведения, принятых в обществе, фиксация наличия или отсутствия конфликтов Участие в мероприятиях

ЛР 30. Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм. ЛР 31. Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности. ЛР 32. Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению. ЛР 33. Принимающий цели и задачи научно-технического, экономического, информационного развития России, готовый работать на их достижение. ЛР 34. Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве. ЛР 35. Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации. ЛР 37. Осуществляющий поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	профессионального мастерства, олимпиадах по профессии, викторинах, в предметных неделях; - готовность к общению и взаимодействию с людьми самого разного статуса, этнической, религиозной принадлежности и в многообразных обстоятельствах; - демонстрация навыков межличностного делового общения, социального имиджа; - проявление мировоззренческих установок на готовность молодых людей к работе на благо Отечества; - проявление правовой активности и навыков правомерного поведения, уважения к Закону; - проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве; - участие в конкурсах профессионального мастерства и в командных проектах; - проявление высокопрофессиональной трудовой активности; - соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, мастерами и руководителями практики	гражданской направленности, в волонтёрских акциях Фиксация наличия или отсутствия правонарушений, наличия или отсутствия постановки на профилактический учёт в органах системы профилактики Проекты, творческие работы, участие в конкурсах и конференциях экологической направленности, участие в экологических субботниках Отсутствие вредных привычек, участие в работе спортивных секций, в спортивных и здоровье сберегающих мероприятиях Наблюдение, мониторинг размещения материалов в социальных сетях Участие в проектах экономической и финансовой направленности, анализ продуктов деятельности