ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Факультет среднего профессионального образования

УТВЕРЖДЕНО
Председатель учебно-методической комиссии факультета СПО, доцент
_____Завершинская М.В.
«____»_____2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12 Безопасность и управление доступом в информационных системах

Специальность09.02. 04 Информационные системы (по отраслям)

Форма обучения очная

Срок получения СПО по ППССЗ 3 года 10 месяцев

Оренбург, 2016г.

1ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12.Безопасность и управление доступом в информационных системах

1.1 Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.04 Информационные системы (по отраслям) утвержденным Министерством образования и науки Российской Федерации 14.05.2014 г., приказ № 525 и зарегистрированным в Минюст России 3 июля 2014. № 32962

1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина «Безопасность и управление доступом в информационных системах» входит в профессиональный учебный цикл.

1.3 Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате изучения дисциплины обучающийся должен уметь:

- применять методы защиты информации в АИС;
- обеспечивать разноуровневый доступ к информационным ресурсам АИС;
- реализовывать политику безопасности в АИС;
- обеспечивать антивирусную защиту информации;

В результате изучения дисциплины обучающийся должен знать:

- сущность информационной безопасности автоматизированных информационных систем (АИС);
- источники возникновения информационных угроз;
- методы защиты информации в АИС;
- модели и принципы защиты информации от несанкционированного доступа;
- приемы организации доступа и управления им в АИС;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации.

1.4 Количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося88 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося60часов;
самостоятельной работы обучающегося28часов.

РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Код	Наименование результата обучения
ПК 1.1	Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.
ПК 1.2	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.
ПК 1.3	Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.
ПК 1.7	Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.
ПК 1.9	Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.
ОК 1	Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**	**V Семестр**	**__Семестр**
Максимальная учебная нагрузка (всего)	**88**	**88**	
Обязательная аудиторная учебная нагрузка (всего)	**60**	**60**	
В том числе:			
аудиторные занятия (лекции)	50	50	
практические занятия (семинарские)	10	10	
Самостоятельная работа обучающегося (всего)	**28**	**28**	
Вопросы , выделенные на самостоятельное изучение	14	14	
рефераты	8	8	
другие виды работ	6	6	
Итоговая аттестация в форме **экзамена**			

2.2 Тематический план и содержание учебной дисциплины ОП.12 Безопасность и управление доступом в информационных системах

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Формируемая компетенция	Уровень освоения
1	2	3		4
Раздел 1. Основы безопасности информационных систем		**12**	ОК 1.	
Введение	Цели и задачи дисциплины. Эволюция подходов к обеспечени мационной безопасности. Роль и место знаний по дисциплине в сфе ссиональной деятельности.	2		1
Тема 1.1.Основные понятия и определения	**Содержание учебного материала**	**4**		1
	Понятие информационной безопасности. Основные принци мационной безопасности: целостность, конфиденциальность, доступнос ты безопасности.	2	ОК 1.	
	Уровни обеспечения информационной безопасности. Определение требований к уровню обеспечения информационной безопасности. Основные составляющие информационной безопасности.	2	ОК 1.	1
Тема 1.2.Угрозы безопасности	**Содержание учебного материала**	**6**		
	Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Информационные, программно-математические, физические и организационные угрозы.	2	ОК 1. ПК 1.2 ПК 1.3	1
	Общие методы обеспечения информационной безопасности: правовые, организационно-технические, экономические. Их сущность, назначение и основные составляющие.	2	ОК 1. ПК 1.2 ПК 1.3	1
	Практическое занятие № 1			
	Информационные, программно-математические, физические и организационные угрозы.	2		2
	Самостоятельная работа обучающихся выполнение домашних заданий по разделу 1	**4**		

	Примерная тематика внеаудиторной самостоятельной работы Основные принципы информационной безопасности: целостность, конфиденциальность, доступность. (конспект) Основные составляющие информационной безопасности (конспект)			
Раздел 2 Защита информации в АИС		**12**		
Тема 2.1 Основные принципы построения подсистемы защиты информации	**Содержание учебного материала**			
	Основные подходы к созданию защиты АИС. Основные функции подсистемы защиты информационной системы. Идентификация и аутентификация. Разграничение доступа. Контроль целостности.	2	ОК 2. ОК 4 ОК 8. ПК 1.2	1
	Основные принципы построения подсистемы защиты информации Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Обнаружение и противодействие атакам. Понятие политики безопасности. Этапы реализации политики безопасности	2	ОК 2. ОК 4 ОК 8.	
Тема 2.2Методы защиты информации.	**Содержание учебного материала**			
	Методы защиты информации в АИС. Организационные, правовы ческие, программно-математические методы и их соотношение.	2	ОК 2. ОК 5	1
	Практическое занятие №2			
	Методы защиты информации в АИС.	2		2
Тема 2.3 Защита информации от несанкционированного доступа	**Содержание учебного материала**			
	Несанкционированный доступ к информации. Источники и пути реализации несанкционированного доступа к информации в АИС.	2		1
	Защита информации от несанкционированного доступа. Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкционированного доступа.	2		1
	Самостоятельная работа обучающихся выполнение домашних заданий по разделу 2	**4**		
	Примерная тематика внеаудиторной самостоятельной работы Криптографические механизмы конфиденциальности, целостности и аутентичности информации.(реферат) Этапы реализации политики безопасности.(конспект)			

Раздел 3 Управление доступом в АИС	**Содержание учебного материала**	**12**		
Тема 3.1 Разграничение доступа к информации в информационных системах	Правила разграничения доступа к элементам защищаемой информации. Способы разграничения доступа к информации. Разграничение доступа по уровням секретности, специальным спискам, матрицам полномочий, мандатам.	2	ОК 2.	1
Тема 3.2 Организация разноуровневого доступа в АИС	**Содержание учебного материала**			1
	Принципы организации разноуровневого доступа в АИС. Понятия клиента, прав доступа, объекта доступа. Учетные записи пользователей АИС. Понятие группы и роли.	2	ОК 2. ОК 6 ОК 7 ОК 8.	1
	Организация разноуровневого доступа в АИС Создание и администрирование групп пользователей. Локальные и глобальные группы пользователей. Понятие политики безопасности в современных АИС.	2	ОК 2. ОК 6 ОК 7 ОК 8.	1
	Практическое занятие №3			2
	Планирование, создание и изменение учетных записей пользователя.	2		1
Тема 3.3 Реализация политики безопасности в АИС	Обеспечение безопасности ресурсов с помощью разрешений NTFS. Разрешения для папок и файлов в NTFS. Множественные разрешения NTFS. Наследование разрешений в NTFS. Планирование, установка и изменение разрешений NTFS . (конспект)	2	ОК 6 ОК 7 ПК 1.3	1
	Изменение параметров учетных записей. Управление группами. Настройк ики безопасности учетных записей. Настройка параметров безопасности ционной системы. Настройка параметров безопасности Интернет.	2	ОК 6 ОК 7 ПК 1.3	1
	Самостоятельная работа обучающихся выполнение домашних заданий по разделу 3	**10**		
	Примерная тематика внеаудиторной самостоятельной работы Изменение параметров учетных записей. (конспект) Учетные записи пользователей АИС. (конспект) Правила разграничения доступа к элементам защищаемой информации (презентация) Способы разграничения доступа к информации. (доклад)			

	Криптографические механизмы конфиденциальности, целостности и аутентичности информации.(реферат)			
Раздел 4 Антивирусная защита информации		**12**		
Тема 4.1 Компьютерные вирусы	**Содержание учебного материала**	2	ОК 3. ОК 5	1
	Понятие компьютерного вируса. Классификация компьютерных вирусов по среде обитания, способу заражения, степени воздействия, особенностям алгоритмов. Сущность и проявление компьютерных вирусов. Структура современных вирусных программ. Программные закладки			
	Основные методы защиты от воздействия вирусов. Общие средства защиты информации. Профилактика вирусного заражения. Специализированные программы для защиты от вирусов.	2	ОК 3.	1
Тема 4.2 Антивирусное программное обеспечение	**Содержание учебного материала**			1
	Методы антивирусной защиты: сигнатурное сканирование, эвристический анализ, контроль целостности, антивирусный мониторинг. Их достоинства и недостатки. вирусных программ. Их характеристика и возможности применения.	2	ОК 3. ПК 1.3 ПК 1.7	1
	Антивирусное программное обеспечение и его классификация. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Современные пакеты антивирусных программ	2	ОК 3. ПК 1.3 ПК 1.7	1
Тема4.3Применение антивирусного программного обеспечения	**Содержание учебного материала**			
	Установка антивирусного программного обеспечения. Приемы работы с антивирусным программным обеспечением. Применение антивирусного программного обеспечения	2	ОК 3. ОК 8. ПК 1.3 ПК 1.7	1
	Практическое занятие №4			2
	Инсталляция и настройка антивирусной программы. Работа с	2		2

	антивирусной программой			
	Самостоятельная работа обучающихся выполнение домашних заданий по разделу 4	**6**		
	Примерная тематика внеаудиторной самостоятельной работы Инсталляция и настройка антивирусной программы. Работа с антивирусной программой (презентация) Приемы работы с антивирусным программным обеспечением.(конспект) Структура современных вирусных программ. Программные закладки (реферат)			
Раздел 5. Организационно - правовое обеспечение ИБ		**12**		
Тема 5.1. Правовое обеспечение информационной безопасности	Концепция правового обеспечения информационной безопасности Российской Федерации. Законодательная база, стандарты и нормативно-методические документы РФ в области обеспечения информационной безопасности. Ответственность за нарушение законодательства в информационной сфере.	2	ОК 4 ОК 9. ПК 1.9	1
	Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью	2	ОК 4 ОК 9. ПК 1.9	1
	Правовое обеспечение информационной безопасности	2	ОК 4 ОК 9. ПК 1.9	1
Тема 5.2. Организационное обеспечение информационной безопасности	Сущность организационной защиты информации и ее место в системе комплексной защиты информации АИС. Организация работ по обеспечению информационной безопасности.	2	ОК 5 ОК 9. ПК 1.1 ПК 1.2 ПК 1.9	1
	Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.	2	ОК 5 ОК 9.	1

			ПК 1.1 ПК 1.2 ПК 1.9	
	Практическое занятие №5			
	Организация работ по обеспечению информационной безопасности	2	2	2
	Самостоятельная работа обучающихся выполнение домашних заданий по разделу 5	2		
	Примерная тематика внеаудиторной самостоятельной работы Организация работ по обеспечению информационной безопасности.(конспект) Порядок создания, утверждения и исполнения должностных инструкций.(реферат)	4		
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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1Требования к минимальному материально-техническому обеспечению

Лаборатория информационных систем:
- компьютерные столы -20 шт.;
- компьютерные стулья – 20 шт.;
-стол учительский – 1 шт.;
-стул учительский – 1 шт;
- компьютеры:

Компьютер № 1
Процессор - Pentium(R) Dual-coreCPUE5300 @ 2.60 GHz; ОЗУ - 3 ГБ; объем HDD -320 ГБ;
Тип операционной системы - 32-разрядная
Лицензионное программное обеспечение:
WindowsServer;
Windows 7 Pro;
Microsoft Visio Pro;
Gimp;
Nvu;
QGIS;
Касперский 6,0;
1С:Предприятие 8,0;
Консультант-Плюс.
Свободно распространяемое программное обеспечение:
OpenOffice;
Lazarus;
Microsoft Project;
7-Zip;
Nanocad;
- проектор мультимедийный – 1 шт.;
- экран – 1шт.

3.2 Информационное обеспечение обучения

Основная литература:
1.Авдошин С.М.Технологии и продукты Microsoft в обеспечении информационной безопасности [электронный курс]: [Текст]/учебник/ С.М.Авдошин.- М.: КноРус, 2016.- 433 с. (электронный ресурс http://www.book.ru/book/918259)

Дополнительная литература:
1.Дюгуров Д.В. Сетевая безопасность на основе серверных продуктов Microsoft[Текст]: курс лекций/ Д.В. Дюгуров. - М.:НОИ Интуит, 2016. – 75с. (электронный ресурс http://www.book.ru/book/918218)
2. Кияев В.И. .Безопасность информационных систем [Текст]: курс лекций/

В.И. Кияев. - М.:НОИ Интуит, 2016. – 192с. (электронный ресурс http://www.book.ru/book/917575)

4КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
применять методы защиты информации в АИС	текущий контроль: оценка решения ситуативных задач, разбора производственных ситуаций, выполнения внеаудиторной самостоятельной работы, выполнения практических работ
обеспечивать разноуровневый доступ к информационным ресурсам АИС	текущий контроль: экспертное наблюдение и оценка выполнения практических работ, тестирование
реализовывать политику безопасности в АИС	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения внеаудиторной самостоятельной работы
обеспечивать антивирусную защиту информации	текущий контроль: устный (и/или письменный) опрос, тестирование
Знания:	
сущность информационной безопасности автоматизированных информационных систем (АИС);	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения внеаудиторной самостоятельной работы
источники возникновения информационных угроз;	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения внеаудиторной самостоятельной работы
методы защиты информации в АИС;	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения практических работ, внеаудиторной самостоятельной работы
модели и принципы защиты информации от несанкционированного доступа;	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения практических работ

приемы организации доступа и управления им в АИС;	текущий контроль: устный (и/или письменный) опрос, тестирование, оценка выполнения внеаудиторной самостоятельной работы, оценка выполнения практических работ
методы антивирусной защиты информации;	текущий контроль: устный (и/или письменный) опрос, тестирование
состав и методы организационно-правовой защиты информации.	текущий контроль: устный (и/или письменный) опрос, оценка выполнения практических работ
	Итоговый **экзамен** по дисциплине

Программа разработана в соответствии с ФГОС СПО по специальности 09.02.04 Информационные системы (по отраслям) утвержденный Министерством образования и науки Российской Федерации 14.05.2014 г., приказ № 525 и зарегистрированный в Минюст России 3 июля 2014 .
№ 32962

Разработала: _____

Программа рассмотрена и одобрена на заседании ПЦК общепрофессиональных дисциплин
протокол № ___ от «___»_____2016 г.
Председатель ПЦК _____

Программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета СПО
протокол № ___ от «___»_____2016 г.

Председатель
учебно-методической комиссии_____ М.В. Завершинская

подпись

ЛИСТ СОГЛАСОВАНИЯ

Состав и содержательно-логические связи
Учебных дисциплин, профессиональных модулей, междисциплинарных курсов, практик, входящих в ОПОП

Коды циклов дисциплин, модулей, практик	**Название циклов, дисциплин, профессиональных модулей, междисциплинарных курсов, практик**	**Содержательно-логические связи**		**Коды формируемых компетенций**	**ФИО и подпись эксперта (работодателя/ преподавателя)**
		Коды учебных дисциплин, модулей, курсов, практик (и их разделы)			
		на которые опирается содержание данной учебной дисциплины/модуля/курса/ практики	**для которых содержание данной дисциплины/модуля/курса/ практики выступает *опорой***		
1	**2**	**3**	**4**	**5**	**6**
ОП.00	**Общепрофессиональные дисциплины *(для СПО)***				
ОП.01	Основы архитектуры, устройство и функционирование вычислительных систем	ОДБ.10	ОП.05, ОП.08, ОП.03	ОК 1-9	
ОП.02	Операционные системы	ОДБ.10	ПМ.02, ПМ.03	ОК 1-9	
ОП.03	Компьютерные сети	ОДБ.10	ПМ.02, ПМ.03	ОК 1-9	
ОП.08	Технические средства информатизации	ОДБ.10	ПМ.01	ОК 1-9	
ОП.10	Безопасность жизнедеятельности	ОДБ.09	ПМ.03	ОК 1-10	
ОП.14	Компьютерная графика	ОДБ.10	ПМ.02	ОК 1-9	
ОП.15	Безопасность и управление доступом в информационных системах	ОП.16	ПМ.01	ОК 1-9	
ПМ.00	**Профессиональные модули**				

ПМ.01	Эксплуатация и модификация информационных систем	ПМ.02, ПМ.03	-	ОК 1-9	
ПМ.02	Участие в разработке информационных систем	ПМ.01, ПМ.03	-	ОК 1-9, ПК 2.1-2.6	
ПМ.03	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	ПМ.01, ПМ.02	-	ОК 1-9, ПК 2.1-2.6	