Министерство сельского хозяйства Российской Федерации
Адамовский сельскохозяйственный техникум-филиал
федерального государственного бюджетного образовательного учреждения
Высшего профессионального образования
«Оренбургский государственный аграрный университет»

УТВЕРЖДАЮ:
Руководитель учебно-методической
комиссии филиала
_____ В.А. Слободяник
«__29__»_____августа____2014 г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 Безопасность и управление доступом в информационных системах

цикл общепрофессиональных дисциплин

программы подготовки специалистов среднего звена

по специальности 09.02.04 Информационные системы (по отраслям)
форма обучения очная

Адамовка 2014 г.

Эксперты:
Внутренняя экспертиза
Техническая экспертиза: Юрченкова Л.В., зав. Методическим кабинетом ФГБОУ ВПО ОГАУ

Содержательная экспертиза: Киселёва С.В., преподаватель ФГБОУ ВПО ОГАУ

Внешняя экспертиза
Содержательная экспертиза: ФИО.,

Рабочая программа разработана в соответствии с разъяснениями по формированию примерных программ учебных дисциплин начального профессионального или среднего профессионального образования, на основе Федеральных государственных образовательных стандартов начального профессионального и среднего профессионального образования, утвержденными И.М. Реморенко, директором Департамента государственной политики и нормативно-правового регулирования в сфере образования Министерства образования и науки Российской Федерации от 27 августа 2009 г.
Содержание программы реализуется в процессе освоения студентами программы подготовки специалистов среднего по специальности 09.02.04 Информационные системы (по отраслям).

ЛИСТ АКТУАЛИЗАЦИИ

№ изменения, дата изменения и № протокола заседания учебно-методической комиссии структурного подразделения СПО, номер страницы с изменением	
БЫЛО	**СТАЛО**
Основание: решение заседания ПЦК от «_____» _____20___ г. Протокол № ____ Председатель _____Киселёва С.В.	

Содержание

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ..... 7

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 13

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.....15

5. Приложение 1…….16

6. Приложение 2…….19

7. Лист согласования…….21

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 Безопасность и управление доступом в информационных системах

1.1. Область применения программы

Рабочая программа учебной дисциплины ОП.14 Безопасность и управление доступом в информационных системах является частью программы подготовки специалистов среднего звена Адамовского сельскохозяйственного техникума филиала ФГБОУ ВПО ОГАУ по специальности 09.02.04 Информационные системы (по отраслям), разработанной в соответствии с ФГОС 3+ СПО.

Рабочая программа разработана для очной формы обучения.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего:

Дисциплина ОП.14 Безопасность и управление доступом в информационных системах входит в вариативную часть общепрофессионального цикла по специальности 09.02.04 Информационные системы (по отраслям).

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

В результате изучения дисциплины студент должен

иметь представление:

– о роли и месте знаний по дисциплине в сфере профессиональной деятельности;

знать:

– основные понятия и определения, эволюция подходов к обеспечению информационной безопасности;
– информационные, программно - математические, физические и организационные угрозы;
– защита от несанкционированного доступа, модели и основные принципы защиты информации;
– принципы организации разноуровневого доступа в автоматизированных информационных системах (АИС);
– понятия клиента, прав доступа, объекта доступа, групп, ролей, политики безопасности в современных АИС;
– проблема вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;
– защита от утечки информации по техническим каналам; организационно-правовое обеспечение информационной безопасности

уметь:

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

Содержание дисциплины ориентировано на подготовку студентов к освоению профессиональных модулей основной профессиональной образовательной программы (ППССЗ) по специальности 09.02.04 Информационные системы (по отраслям) и овладению профессиональными компетенциями (ПК):

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.

В процессе освоения дисциплины формируются общие компетенции (ОК):

ОК 1. Понимать сущность и социальную значимость своей будущей 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. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за

результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Быть готовым к смене технологий в профессиональной деятельности

4. Рекомендуемое количество часов на освоение примерной программы учебной дисциплины:

- максимальной учебной нагрузки обучающегося 88 часов, в том числе:
- обязательной аудиторной учебной нагрузки обучающегося 60 часов;
- самостоятельной работы обучающегося 28 часов.

СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов	Семестр 5
Максимальная учебная нагрузка (всего)	*88*	*88*
Обязательная аудиторная учебная нагрузка (всего)	*60*	*60*
Теоретическая часть	*48*	*48*
Лабораторные практические работы	*10*	*10*
Рубежный контроль	*2*	*2*
Самостоятельная работа обучающегося (всего)	*28*	*28*
в том числе:		
Индивидуальное задание Написание сообщений Составление тестов	*12* *10* *6*	*12* *10* *6*
Итоговая аттестация в форме	*Диф.зачёт*	*Диф.зачёт*

2.2. Примерный тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*	Объем часов		Уровень освое-ния
1	**2**	**3**		**4**
Введение	***Содержание материала.*** 1.Цели и задачи дисциплины. 2.Эволюция подходов к обеспечению информационной безопасности. 3.Роль и место знаний по дисциплине в сфере профессиональной деятельности.	2	ПК 1.1 ПК 1.2	1
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся подготовка рефератов	0,3		
Раздел 1 Основы безопасности информационных систем				*3*
Тема 1.1 Основные понятия и определения	***Содержание материала.*** 1. Понятие информационной безопасности. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность.	*2*	ПК 1.1 ПК 1.3	
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить презентацию по теме «Основные принципы информационной безопасности»	*1,3*		
Тема 1.2 Угрозы безопасности.	***Содержание материала.*** Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Информационные, программно-математические, физические и организационные угрозы	*2*	ПК 1.1 ПК 1.2	*2*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Заполнить таблицу: угрозы информационной безопасности	*1*		
Раздел 2 Защита информации в АИС				
Тема 2.1 Основные принципы построения подсистемы защиты информации.	***Содержание материала.*** 1. Основные подходы к созданию защиты АИС. Основные функции подсистемы защиты информационной системы. Идентификация и аутентификация. Разграничение доступа. Контроль целостности.	*2*	ПК 1.1 ПК 1.7	*2*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить вопросы для перекрестного опроса	1		

Тема 2.2 Основные принципы построения подсистемы защиты информации.	***Содержание материала.*** Обнаружение и противодействие атакам. Понятие политики безопасности	*2*	ПК 1.1	*1*
	Лабораторные работы			
	Практические занятия			
	Контрольные работы			
	Самостоятельная работа обучающихся Подготовить презентацию на тему « защита информации»	*0,3*		
Тема 2.3 Методы защиты информации	***Содержание материала*** Методы защиты информации в АИС. Организационные, правовые, технические, программно-математические методы и их соотношение.	6	ПК 1.1 ПК 1.3	*1*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Составить кроссворд по теме: Методы защиты информации в АИС. 2. Подготовить тест на сопоставление. 3. Подготовить вопросы для перекрестного опроса.	*2,8*		
Тема 2.4 Защита информации от несанкционированного доступа.	***Содержание материал*** Несанкционированный доступ к информации. Источники и пути реализации несанкционированного доступа к информации в АИС.	2	ПК 1.1 ПК 1.9	1
	Лабораторные работы			
	Практические занятия			
	Контрольные работы			
	Самостоятельная работа обучающихся *Подготовить презентацию «Методы защиты информации»*	*0,3*		
Тема 2.5 Защита информации от несанкционированного доступа .	***Содержание материал*** 1. Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкционированного доступа	*2*	ПК 1.1 ПК 1.2	*1*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить реферат по теме: Принципы защиты информации от несанкционированного доступа. 2. Рубежный контроль	*3* 1		
Раздел 3 Управление доступом в АИС				
Тема 3.1 Разграничение доступа к информации в информационных системах.	***Содержание материал*** 1.Правила разграничения доступа к элементам защищаемой информации. Способы разграничения доступа к информации. 2. Разграничение доступа по уровням секретности, специальным спискам, матрицам полномочий, мандатам.	*2*	ПК 1.1	*1*
	Лабораторные работы	-		
	Практические занятия	-		

	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить сообщение по теме: Разграничение доступа к информации в информационных системах.	*2*		
Тема 3.2 Организация разно уровневого доступа в АИС.	***Содержание материал*** 1.Принципы организации разно уровневого доступа в АИС. Понятия клиента, прав доступа, объекта доступа. Учетные записи пользователей АИС.	*2*	ПК 1.1 ПК 1.3	*2*
	Лабораторные работы *1.* Планирование, создание и изменение учетных записей пользователей *2.* Создание и администрирование групп пользователей	*4*		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить кроссворд по теме: Организация разноуровневого доступа в АИС.	*2*		
Тема 3.3 Реализация политика безопасности в АИС	***Содержание материал*** 1. Обеспечение безопасности ресурсов с помощью разрешений NTFS. Разрешения для папок и файлов в NTFS. Множественные разрешения NTFS. Наследование разрешений в NTFS. 2. Планирование, установка и изменение разрешений NTFS. Изменение параметров учетных записей. Управление группами. Настройка политики безопасности учетных записей	*4*	ПК 1.1 ПК 1.7	*2*
	Лабораторные работы 1. Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам. 2. Изменение параметров учетных записей пользователей.	*4*		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить вопросы для перекрестного опроса по теме: Реализация политики безопасности в АИС.	*2*		
Раздел 4 Антивирусная защита информации				
Тема 4.1 Компьютерные вирусы	***Содержание материал*** 1. Понятие компьютерного вируса. Классификация компьютерных вирусов по среде обитания, способу заражения, степени воздействия, особенностям алгоритмов. 2. Сущность и проявление компьютерных вирусов. Структура современных вирусных программ. Программные закладки.	*3*	ПК 1.1 ПК 1.9	*2*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить сообщение по теме: Классификация компьютерных вирусов. 2. Подготовить реферат по теме: Компьютерные вирусы.	*4*		

Тема 4.2 Антивирусное программное обеспечение	***Содержание материал*** 1. Методы антивирусной защиты: сигнатурное сканирование, эвристический анализ, контроль целостности, антивирусный мониторинг. Их достоинства и недостатки.	*4*	ПК 1.1 ПК 1.2	*2*
	Лабораторные работы Работа с антивирусной программой	*2*		
	Практические занятия	-		
	Контрольные работы	--		
	Самостоятельная работа обучающихся 1. Заполнить таблицу по теме: Методы антивирусной защиты: достоинства и недостатки.	*1*		
Тема 4.3 Применение антивирусного программного обеспечения	***Содержание материал*** 1. Установка антивирусного программного обеспечения. Приемы работы с антивирусным программным обеспечение	*2*	ПК 1.1 ПК 1.9	*2*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся	-		
Раздел 5. Организационно-правовое обеспечение информационной безопасности				*1*
Тема 5.1 Правовое обеспечение информационной безопасности	***Содержание материал*** 1. Концепция правового обеспечения информационной безопасности Российской Федерации. Законодательная база, стандарты и нормативно-методические документы РФ в области обеспечения информационной безопасности	*4*	ПК 1.1 ПК 1.7	
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить вопросы для перекрестного опроса. 2. Подготовить сообщение по теме: Концепция правового обеспечения информационной безопасности Российской Федерации.	*4*		
Тема 5.2 Организационное обеспечение информационной безопасности.	***Содержание материал*** 1. Сущность организационной защиты информации и ее место в системе комплексной защиты информации АИС. 2. Организация работ по обеспечению информационной безопасности	*4*	ПК 1.1 ПК 1.3	*2*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся 1. Подготовить тест на сопоставление. 2. Составить кроссворд по теме: Организационное обеспечение информационной безопасности.	*2*		

Тема 5.3 Методы и формы организационной защиты информации	***Содержание материал*** 1. Методы и формы организационной защиты информации. 2. Сущность организационных методов защиты информации.	*3*	ПК 1.1 ПК 1.9	*1*
	Лабораторные работы	-		
	Практические занятия	-		
	Контрольные работы	-		
	Самостоятельная работа обучающихся Дифференцированный зачёт	- *1*		
Тематика курсовой работы (проекта) *(если предусмотрены)*		-		
Самостоятельная работа обучающихся над курсовой работой (проектом) *(если предусмотрены)*		-		
Всего: максимальной учебной нагрузки обучающегося: обязательной аудиторной учебной нагрузки обучающегося; самостоятельной работы обучающегося. **рубежный контроль**		88 58 28 2		

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

Реализация учебной дисциплины требует наличия лабораторий :

1. Информатики и электронно-вычислительных машин
2. Информатики и информационных технологий в профессиональной деятельности

Оборудование лаборатории и рабочих мест лаборатории:

- персональный компьютер Pentium(R) Dual-Core CPU,
- локальная сеть,
- макет внутреннего устройства компьютера,
- прикладное программное обеспечение: Операционная система Windows7,

Приводится перечень средств обучения, включая тренажеры, модели, макеты, оборудование, технические средства, в т. ч. аудиовизуальные, компьютерные и телекоммуникационные и т. п. (Количество не указывается).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Для студента

Основные источники:

[1] Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие для студентов учреждений среднего профессио¬нального образования. - М: ФОРУМ: ИНФРА-М, 2011.- 432 стр.

Дополнительные источники:

ЭБС «Книгофонд» http://www.knigafund.ru

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства (Электронный ресурс) / Шаньгин В.Ф. –М.: ДМК.Пресс.,2010-544с.:ил.
2. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. (Электронный ресурс)/ Сердюк В.А.- Издательство: Издательский дом Государственного университета – Высшей школы экономики, 2011 г.574 страницы

Интернет ресурсы

ЭБС «Книгофонд» http://www.knigafund.ru

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства (Электронный ресурс) / Шаньгин В.Ф. –М.: ДМК.Пресс.,2010-544с.:ил.
4. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. (Электронное ресурс)/ Сердюк В.А.- Издательство: Издательский дом Государственного университета – Высшей школы экономики, 2011 г.574 страницы

Для преподавателя:

Основные источники:

1. [1] Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие для студентов учреждений среднего профессио¬нального образования. - М: ФОРУМ: ИНФРА-М, 2011.- 432 стр.

Дополнительные источники:

ЭБС «Книгофонд» http://www.knigafund.ru

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства (Электронный ресурс) / Шаньгин В.Ф. –М.: ДМК.Пресс.,2010-544с.:ил.
3. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. (Электронный ресурс)/ Сердюк В.А.- Издательство: Издательский дом Государственного университета – Высшей школы экономики, 2011 г.574 страницы

Интернет ресурсы

ЭБС «Книгофонд» http://www.knigafund.ru

4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства (Электронный ресурс) / Шаньгин В.Ф. –М.: ДМК.Пресс.,2010-544с.:ил.
5. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. (Электронное ресурс)/ Сердюк В.А.- Издательство: Издательский дом Государственного университета – Высшей школы экономики, 2011 г.574 страницы

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам усвоения дисциплины.

Текущий контроль проводиться в форме : письменной контрольной работы, тестирования, индивидуальные и фронтальные опросы.

Промежуточная аттестация проводится в форме дифференцированного зачёта.

Методическое обеспечение в виде перечня вопросов для экзамена, содержания контрольных работ, тестовых заданий отражено в учебно-методическом комплексе по дисциплине.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения учебной дисциплины обучающийся должен уметь:	
- применять методы защиты информации в АИС;	*Устный опрос (фронтальный , индивидуальный, комбинированный)*
- обеспечивать разноуровневый доступ к информации онным ресурсам АИС;	*Практическое задание* *Диф. зачёт*
- реализовывать политику безопасности в АИС;	*Практическое задание*
- обеспечивать антивирусную защиту информации.	*Практическое занятие*
В результате освоения учебной дисциплины обучающийся должен знать:	
- основные понятия и определения, эволюция подходов к обеспечению информационной безопасности;	*Устный комбинированный опрос* *Рецензирование ответов*
- информационные, программно - математические, физические и организационные угрозы;	*Тестирование* *Практическое занятие*
- защита от несанкционированного доступа, модели и основные принципы защиты информации;	*Устный опрос (фронтальный , индивидуальный, комбинированный)*
- принципы организации разноуровневого доступа в автоматизированных информационных системах (АИС);	Тестирование
- проблема вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;	Практическое занятие Тестирование
- защита от утечки информации по техническим каналам; организационно-правовое обеспечение информационной безопасности деятельности;	Дифференцированный зачет

ПРИЛОЖЕНИЕ 1

КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ВПД - Эксплуатация и модификация информационных систем	
Уметь: - обеспечивать антивирусную защиту информации - обеспечивать разноуровневый доступ к информационным ресурсам АИС; - реализовывать политику безопасности в АИС; - применять методы защиты информации в АИС;	**Тематика лабораторных/практических работ, формирующие умение и направленные на подготовку ПК**: ЛР№1: Вирусы и антивирусы ЛР№2: Использование антивирусов как средство защиты информации; ЛР№3:Создание учётной записи пользователя ; ЛР№4: Создание и администрирование групп пользователей; ЛР№5: Изменение параметров учётных записей пользователя ;
Знать: -основные понятия и определения, эволюция подходов к обеспечению информационной безопасности; - информационные, программно - математические, физические и организационные угрозы; -защита от несанкционированного доступа, модели и основные принципы защиты информации;	**Перечень тем:** Понятие информационной безопасности. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Информационные, программно-математические, физические и организационные угрозы Основные подходы к созданию защиты АИС. Основные функции подсистемы защиты информационной системы. Идентификация и аутентификация. Разграничение доступа. Контроль целостности Обнаружение и противодействие атакам. Понятие политики безопасности Методы защиты информации в АИС. Организационные, правовые, технические, программно-математические методы и их соотношение Несанкционированный доступ к информации. Источники и пути реализации несанкционированного доступа к информации в АИС Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкциониро-

	ванного доступа
-принципы организации разноуровневого доступа в автоматизированных информационных системах (АИС);	Правила разграничения доступа к элементам защищаемой информации. Способы разграничения доступа к информации. Разграничение доступа по уровням секретности, специальным спискам, матрицам полномочий, мандатам
-понятия клиента, прав доступа, объекта доступа, групп, ролей, политики безопасности в современных АИС;	Принципы организации разно уровневого доступа в АИС. Понятия клиента, прав доступа, объекта доступа. Учетные записи пользователей 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. Изменение параметров учетных записей. Управление группами. Настройка политики безопасности учетных записей
-проблема вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты;	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. Методы антивирусной защиты: сигнатурное сканирование, эвристический анализ, контроль целостности, антивирусный мониторинг. Их достоинства и недостатки.
-защита от утечки информации по техническим каналам;	Установка антивирусного программного обеспечения. Приемы работы с антивирусным программным обеспечение
- организационно-правовое обеспечение информационной безопасности	Концепция правового обеспечения информационной безопасности Российской Федерации. Законодательная база, стандарты и нормативно-методические документы РФ в области обеспечения информационной безопасности Сущность организационной защиты информации и ее место в системе комплексной защиты информации АИС. Организация работ по обеспечению информационной безопасности Методы и формы организационной защиты информации. Сущность организационных методов защиты информации
Самостоятельная работа студента	**Тематика самостоятельной работы**: Проработка конспекта по пройденным темам; Подготовка презентации на темы: - Основные принципы информационной безопасности - Защита информации - Методы защиты информации Подготовка сообщений на темы: - Разграничение доступа к информации в информационных

	системах. - Классификация компьютерных вирусов. - Концепция правового обеспечения информационной безопасности Российской Федерации Выполнение рефератов на тему: - Принципы защиты информации от несанкционированного доступа - Компьютерные вирусы

Приложение 2

ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ОК

Название ОК	**Технологии формирования ОК (на учебных занятиях)**
ОК.1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	Мотивация учебной деятельности с использованием примеров (успешные выпускники);
ОК.2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Используются задания для самостоятельной работы (подготовка сообщений, презентаций; индивидуальные задания)
ОК.3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	Используется направление деятельности: Демократичное влияние на решение каждым студентом личных проблем: «вести или не вести записи (конспект) при объяснениях преподавателя», «при выполнении ЛР быть наблюдателем или исполнителем», …
ОК.4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Используются задания для самостоятельной работы (индивидуальные задания на составление собственных «баз данных»)
ОК.5. Владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий.	Используются задания для самостоятельной работы Поиск информации в Интернете для подготовки сообщений, презентаций по изучаемой теме.
ОК.6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	Используется направление деятельности: «каждый член звена – активный участник при выполнении лабораторных работ; при коллективной деятельности». …
ОК.7. Ставить цели, мотивировать деятель-	Организация групп на лабораторных заня-

ность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий	тиях и назначение ответственного за результат деятельности группы.
ОК.8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Используются задания для самостоятельной работы (подготовка сообщений, презентаций).
ОК.9. Быть готовым к смене технологий в профессиональной деятельности.	Используется направление деятельности: Лекции, лабораторные работы, участие в реализации различных проектов во внеаудиторной деятельности

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		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 учебной дисциплины модуля/ курса/ практики выступает опорой	
1	2	3	4	5
ОП	**Обще профессиональных**			
ОП.15	Безопасность и управление доступом в информационных системах	«Операционные системы и среды»		
		«Компьютерные сети»		
			Основы проектирования баз данных	

Авторы: Остапчук Ю.А. преподаватель АСХТ филиала ФГБОУ ВПО ОГАУ

Рецензенты: Киселёва С.В. преподаватель ЦК естественно математических дисциплин

Программа рассмотрена и одобрена на заседании ЦК
_____естественно математических дисциплин_____
(наименование ЦК)

Протокол №___1___ от «27»_августа__2014_г.

Председатель ЦК _____ С.В.Киселёва

Программа рассмотрена и одобрена на заседании учебно-методической комиссии филиала

Протокол №___1___ от «29»_августа__2014__г.

Зав.методическим кабинетом _____ Л.В. Юрченкова

Согласовано с заведующей библиотекой филиала _____ Т.М. Крат