БУЗУЛУКСКИЙ ГИДРОМЕЛИОРАТИВНЫЙ ТЕХНИКУМ – ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО

Председатель учебно-методической комиссии БГМТ- филиала ФГБОУ ВО Оренбургский ГАУ
Евсюков С.А
«27» марта 2018г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## ОП.12 БЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ ДОСТУПОМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Специальность** 09.02.04 Информационные системы ( по отраслям)

**Форма обучения** очная

**Срок получения СПО по ППССЗ** 3года 10 месяцев

Бузулук, 2018 г.

**СОДЕРЖАНИЕ**

**ЛИСТ АКТУАЛИЗАЦИИ**

| № изменения, дата изменения и № протокола заседания учебно-методической комиссии филиала, номер страницы с изменением | |
|---|---|
| БЫЛО | СТАЛО |
| Основание: решение заседания ПЦК специальности 09.02.04 Информационные системы (по отраслям) от «___»_____№_____протокола<br>_____ Мартынова Е.Н., председатель ПЦК<br>*подпись* | |

## 1 ПАСПОРТ РАБОЧЕЙ 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 программы подготовки специалиста среднего звена

Дисциплина «Безопасность и управление доступом в информационных системах» входит в профессиональный 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 информационных систем;
- 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 рабочей программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося 122 часа, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 82 часа;
самостоятельной работы обучающегося 40 часов.

## 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 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. | 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 УЧЕБНОЙ ДИСЦИПЛИНЫ

## 2.1 Объем учебной дисциплины и виды учебной работы

| Вид учебной работы | Объем часов | 5 Семестр |
|---|---|---|
| **Максимальная учебная нагрузка (всего)** | **122** | **122** |
| **Обязательная аудиторная учебная нагрузка (всего)** | **82** | **82** |
| В том числе: | | |
| лекции, уроки | 72 | 72 |
| практические занятия | 10 | 10 |
| **Самостоятельная работа обучающегося (всего)** | **40** | **40** |
| **Промежуточная 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** | | **22** | | |
| Введение | Цели и задачи дисциплины. Эволюция подходов к обеспечению информационной безопасности. Роль и место знаний по дисциплине в сфере профессиональной деятельности. | 2 | | 1 |
| Тема 1.1.Основные понятия и определения | **Содержание учебного материала** | | | 1 |
| | Понятие информационной безопасности. Объекты безопасности. | 2 | ОК 1. | 1 |
| | Основные принципы информационной безопасности: целостность, конфиденциальность, доступность. | 2 | ОК 1. | 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** | | | |
| | Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. | 2 | ОК 2. | 1 |
| | Информационные, программно-математические, физические и организационные угрозы. | 2 | ОК 2. | |
| | Общие методы обеспечения информационной безопасности: правовые, организационно-технические, экономические. Их сущность, назначение и основные составляющие. | 2 | ОК 2. | 1 |
| | **Практическое занятие № 1** | | | |
| | Информационные, программно-математические, физические и | 2 | ОК 2. | 2 |

| | | | | |
|---|---|---|---|---|
| | организационные угрозы. | | | |
| | **Самостоятельная работа обучающихся** выполнение домашних заданий по разделу 1 | **6** | | |
| | **Тематика внеаудиторной самостоятельной работы**<br>Основные принципы информационной безопасности: целостность, конфиденциальность, доступность. (презентация) – 2ч.<br>Основные составляющие информационной безопасности (презентация) – 2ч.<br>Закон РФ «Об участии в международном информационном обмене» (презентация) – 2ч. | | | |
| **Раздел 2 Защита информации в АИС** | | **28** | | |
| 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, аутентификация, авторизация. | 2 | ОК 4. | 1 |
| | Разграничение доступа. Контроль целостности.<br>Основные принципы построения подсистемы защиты информации | 2 | ОК 4. | 1 |
| | Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Структура скриптосистемы. Классификация систем шифрования данных. | 2 | ОК 4. | 1 |
| | Симметричные и асимметричные методы шифрования<br>Механизм электронной цифровой подписи | 2 | ОК 4. | 1 |
| | Обнаружение и противодействие атакам. Понятие политики безопасности. Этапы реализации политики безопасности | 2 | ОК 4. | 1 |
| Тема 2.2 Методы защиты информации. | **Содержание учебного материала** | 2 | | 1 |
| | Методы защиты информации в АИС. Организационные, правовые методы защиты информации. | | ОК8. | |
| | Методы защиты информации и их соотношение в АИС. Технические, | 2 | ОК8. | 1 |

| | | | | |
|---|---|---|---|---|
| | программно-математические методы. | | | |
| | **Практическое занятие №2** | | | |
| | Методы защиты информации в АИС. | 2 | ОК8. | 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 | ОК 9. | 1 |
| | Защита информации от несанкционированного доступа. Основные принципы защиты информации от несанкционированного доступа. Средства и механизмы защиты от несанкционированного доступа. | 2 | ОК 9. | 1 |
| | **Самостоятельная работа обучающихся** выполнение домашних заданий по разделу 2 | **8** | | |
| | **Тематика внеаудиторной самостоятельной работы**<br>Криптографические механизмы конфиденциальности, целостности и аутентичности информации. (реферат) - 2ч.<br>Этапы реализации политики безопасности. (реферат) – 2ч.<br>Средства защиты информации. (реферат) – 2ч.<br>Угроза информационной безопасности (реферат) – 2ч. | | | |
| **Раздел 3 Управление доступом в АИС** | **Содержание учебного материала** | **32** | | |
| 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 | ПК 1.1. | 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. | 2 | ОК 6.;<br>ОК 7. | 1 |
| | Учетные записи пользователей АИС. Понятие группы и роли. | 2 | ОК 6.; ОК 7. | 1 |
| | Организация разноуровневого доступа в АИС Создание и администрирование групп пользователей. Локальные и глобальные | 2 | ОК 6.; ОК 7. | 1 |

| | | | | |
|---|---|---|---|---|
| | группы пользователей. Понятие политики безопасности в современных АИС. | | | |
| | **Практическое занятие №3** | | ОК 6.; ОК 7. | 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 . | 2 | ПК 1.2. | 1 |
| | Изменение параметров учетных записей. Управление группами. Настройка политики безопасности учетных записей. | 2 | ПК 1.2. | 1 |
| | Настройка параметров безопасности операционной системы. Настройка параметров безопасности Интернет. | 2 | ПК 1.2. | 1 |
| | **Самостоятельная работа обучающихся** выполнение домашних заданий по разделу 3 | **16** | | |
| | **Тематика внеаудиторной самостоятельной работы**<br>Изменение параметров учетных записей. (конспект) – 2ч.<br>Учетные записи пользователей АИС. (конспект) – 2ч.<br>Определение и содержание регистрации и аудита информационных систем (конспект) – 2ч.<br>Правила разграничения доступа к элементам защищаемой информации (конспект) – 2ч.<br>Способы разграничения доступа к информации. (конспект) – 2ч.<br>Криптографические механизмы конфиденциальности, целостности и аутентичности информации.(конспект) - 2ч.<br>История криптографии (конспект) – 2ч.<br>Файловой системы FAT (конспект) – 2ч. | | | |
| **Раздел 4 Антивирусная защита информации** | | **22** | | |
| Тема 4.1 | **Содержание учебного материала** | | | 1 |

| | | | | |
|---|---|---|---|---|
| Компьютерные вирусы | Понятие компьютерного вируса. Классификация компьютерных вирусов по среде обитания, способу заражения, степени воздействия, особенностям алгоритмов. Сущность и проявление компьютерных вирусов. | 2 | ПК 1.3. | |
| | Структура современных вирусных программ. Программные закладки | 2 | ПК 1.3. | 1 |
| | Основные методы защиты от воздействия вирусов. Общие средства защиты информации. Профилактика вирусного заражения. Специализированные программы для защиты от вирусов. | 2 | ПК 1.3. | 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. | 2 | ОК 3. | 1 |
| | Антивирусное программное обеспечение и его классификация. Программы-детекторы, программы-доктора. | 2 | ОК 3. | 1 |
| | Антивирусное ПО. Программы-ревизоры, программы-фильтры. Современные пакеты антивирусных программ. | 2 | ОК 3. | 1 |
| Тема4.3 Применение 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 антивирусной программой | 2 | | 2 |
| | **Самостоятельная работа обучающихся** выполнение домашних заданий по разделу 4 | **6** | | |
| | **Тематика внеаудиторной самостоятельной работы**<br>Инсталляция и настройка антивирусной программы. Работа с антивирусной программой (конспект) – 2ч.<br>Приемы работы с антивирусным программным обеспечением(конспект) – 2ч.<br>Структура современных вирусных программ. Программные | | | |

| | | | | |
|---|---|---|---|---|
| | закладки (презентация) – 2ч. | | | |
| **Раздел 5. Организационно - правовое обеспечение информационной безопасности** | | **18** | | |
| 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 | ПК 1.7. | 1 |
| | Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью | 2 | ПК 1.7. | 1 |
| | Правовое обеспечение информационной безопасности | 2 | ПК 1.7. | 1 |
| Тема 5.2. Организационное обеспечение информационной безопасности | Сущность организационной защиты информации и ее место в системе комплексной защиты информации АИС.. | 2 | ПК 1.9.; ОК 5. | 1 |
| | Организация работ по обеспечению информационной безопасности | 2 | ПК 1.9.; ОК 5. | 1 |
| | Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций. | 2 | ПК 1.9.; ОК 5. | 1 |
| | **Практическое занятие №5** | | ПК 1.9.; ОК 5. | |
| | Организация работ по обеспечению информационной безопасности | 2 | | 2 |
| | **Самостоятельная работа обучающихся** выполнение домашних заданий по разделу 5 | 4 | | |
| | **Тематика внеаудиторной самостоятельной работы**<br>Порядок создания, утверждения и исполнения должностных инструкций. ( конспект) – 2ч. | | | |

| | | | | |
|---|---|---|---|---|
| | Организационная защита на предприятиях (конспект) – 2ч. | | | |
| **Всего:** | | **122** | | |

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 РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 3.1Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия лаборатории информационных систем:

- компьютерные столы -12 шт.;
- компьютерные стулья – 12 шт.;
-стол учительский – 1 шт.;
-стул учительский – 1 шт;
- сплит- система;
- компьютеры - 12:
- мультимедийный проектор – 1 шт.;
- экран – 1шт.;

Наглядные учебные пособия:
Компьютер и информация -1 шт.
Устройство компьютера – 1 шт.
Компьютер и безопасность -1 шт
Лицензионное программное обеспечение:
Windows 7 Pro;
Microsoft Visio Pro;
Касперский Endpoint Security 10;
Свободно распространяемое лицензионное программное обеспечение:
Gimp;
Nvu;
QGIS
Open Office;
OpenProj;
UMLet;
Free Pascal;
Lazarus;
VirtualBox
7-Zip;
Nanocad;
Eclipse
Adobe Acrobat Reader;

### 3.2 Информационное обеспечение обучения

**Основная литература:**

1.Васильков А. В. Безопасность и управления доступом в информационных системах [Текст]: учебное пособие/А. В. Васильков – М.: ФОРУМ: ИНФРА-М, 2016.-368с.
2. Нестеров С. А. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессиональное образование) https://biblio-online.ru/book/1997F695-44FF-4570-BF5D-882F5286AE77/informacionnaya-bezopasnost

**Дополнительная литература:**

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие/В. Ф. Шаньгин.- М.: ФОРУМ: ИНФРА-М, 2014.-416с.

## 4 КОНТРОЛЬ 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 информационных систем; | 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 |
| | **Экзамен** |

Программа разработана в соответствии с ФГОС СПО по специальности 09.02.04 Информационные системы (по отраслям), утверждённым Министерством образования и науки Российской Федерации 14.05.2014 г., приказ № 525 и зарегистрированным в Минюсте России 3.07.2014г., № 32962

Разработала: _____ Марисова А.П.
*подпись*

Программа рассмотрена и одобрена на заседании ПЦК специальности 09.02.04 Информационные системы (по отраслям)

протокол № 8 от «23» марта 2018 г.

Председатель ПЦК _____ Мартынова Е.Н.
*подпись*

Программа рассмотрена и одобрена на заседании учебно- методической комиссии БГМТ- филиала ФГБОУ ВО Оренбургский ГАУ

протокол № 7 от «27» марта 2018г.

Председатель учебно-методической комиссии _____ Евсюков С.А.
*подпись*

СОГЛАСОВАНО

Методист филиала _____ Леонтьева Е.Р.
*подпись*

Заведующая библиотекой _____ Дмитриева Н.М.
*подпись*