

## АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

**Разработчик:** Марисова А.П.

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

**Наименование 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 и направлена на формирование соответствующих общих, профессиональных компетенций.

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.

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 установку 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.

### **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.

Форма аттестации - 5 семестр – экзамен

#### **1.5 Содержание учебной дисциплины**

Введение

*Раздел 1. Основы безопасности информационных систем*

Введение

Тема 1.1. Основные понятия и определения

Тема 1.2. Угрозы безопасности

*Раздел 2 Защита информации в АИС*

Тема 2.1 Основные принципы построения подсистемы защиты информации

Тема 2.2 Методы защиты информации

Тема 2.3 Защита информации от несанкционированного доступа

*Раздел 3 Управление доступом в АИС*

Тема 3.1 Разграничение доступа к информации в информационных системах

Тема 3.2 Организация разноуровневого доступа в АИС

Тема 3.3 Реализация политики безопасности в АИС

*Раздел 4 Антивирусная защита информации*

Тема 4.1 Компьютерные вирусы

Тема 4.2 Антивирусное программное обеспечение

Тема 4.3 Применение антивирусного программного обеспечения

*Раздел 5. Организационно - правовое обеспечение информационной*

*безопасности*

Тема 5.1 Правовое обеспечение информационной безопасности

Тема 5.2 Организационное обеспечение информационной безопасности