

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Саратовский государственный технический университет  
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

## АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине Б.1.1.23 «Основы управления информационной  
безопасностью»

направления подготовки

10.03.01 «Информационная безопасность»

Профиль «Безопасность автоматизированных систем»

форма обучения – очная

курс – 4

семестр – 8

зачетных единиц – 2

часов в неделю – 2

всего часов – 72

лекции – 16

коллоквиумы - 2

практические занятия – 18

самостоятельная работа – 36

зачет – 8 семестр

## 1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачи изучения дисциплины:

- 1) изучение основных понятий и методологий управления информационной безопасностью;
- 2) получение знаний и навыков в области оценки рисков информационной безопасности;
- 3) изучение методологии проведения аудита информационной безопасности;
- 4) приобретение обучаемыми необходимого объема знаний в области организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
- 5) формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

## 2. Место дисциплины в структуре ООП ВО

Дисциплина «Основы управления информационной безопасностью» относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Знания и практические навыки, полученные при изучении дисциплины «Основы управления информационной безопасностью», используются при написании итоговой аттестационной работы.

### **3. Требования к результатам освоения дисциплины**

Изучение дисциплины направлено на формирование следующих компетенций:

способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

Студент должен знать:

– значение управлением информационной безопасностью в условиях развития современного общества;

– содержание основных нормативно-правовых актов, регламентирующих вопросы в сфере управления информационной безопасностью;

– процедуры организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Студент должен уметь:

– применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

– применять нормативные правовые акты и нормативные методические документы в сфере управления информационной безопасностью;

– классифицировать действующие нормативные и методические документы ФСТЭК России, ФСБ России и Роскомнадзора в соответствии с их полномочиями;

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

- разрабатывать частные политики информационной безопасности информационных систем;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем.

Студент должен владеть навыками:

- навыками формирования требований по защите информации;
- навыками работы с нормативными правовыми актами в области управления информационной безопасностью;
- навыками работы с технологиями поиска нормативных правовых актов и нормативных методических документов в области управления информационной безопасностью в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;
- навыками мониторинга и аудита, выявления угроз информационной безопасности;
- навыками формирования требований по защите информации;
- методами управления информационной безопасностью.