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 С.1.1.30 «Управление информационной безопасности»

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
Специализация «Создание автоматизированных систем
в защищенном исполнении»

форма обучения – очная
курс – 5
семестр – 9
зачетных единиц – 3
часов в неделю – 3
всего часов – 108
лекции – 18
практические занятия – 36
самостоятельная работа – 54
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 «Управление 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 «Управление информационной безопасностью», используются при написании итоговой аттестационной работы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

способность управлять информационной безопасностью автоматизированной системы (ПК-28)

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 поиска и обработки нормативные правовые акты и нормативные методические документы в области управления информационной безопасности;

– основные принципы аудита информационной безопасности;

– принципы формирования политики информационной безопасности в автоматизированных системах;

– основные методы (правила, процедуры, практические приемы и пр.) управления информационной безопасностью.

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 информационной безопасности автоматизированных систем;

– определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем.

Студент должен владеть навыками:

– навыками формирования требований по защите информации;

– навыками работы с нормативными правовыми актами в области управления информационной безопасности;

– навыками работы с технологиями поиска нормативных правовых актов и нормативных методических документов в области управления информационной безопасности 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.