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.3.2.5 «Комплексное обеспечение информационной безопасности автоматизированных систем»*

направления подготовки
*10.03.01 "Информационная безопасность"*
*Профиль "Безопасность автоматизированных систем"*

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 6
часов в неделю – 5
всего часов – 216,
в том числе:
лекции – 32
коллоквиумы – 4
лабораторные занятия – 54
самостоятельная работа – 126
курсовая работа – 7 семестр
экзамен – 7 семестр

## 1. Цели и задачи дисциплины

Цель преподавания дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»: подготовка студентов к деятельности по созданию систем информационной безопасности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, на базе комплексного подхода применения правил, процедур, практических приемов, руководящих принципов, методов, средств обеспечения информационной безопасности.

Задачи изучения дисциплины:

сформировать способность к комплексному применению мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированной системы.

## 2. Место дисциплины в структуре ООП ВПО

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к числу дисциплин вариативной части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Техническая защита информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Разработка и эксплуатация защищенных автоматизированных систем» .

Знания, умения и навыки, сформированные при изучении дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» необходимы при выполнении выпускной квалификационной работы.

## 3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-3 способность использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4 способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5 способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;
ПК-7 способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
ПК-9 способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;
ПК-25 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
ПК-26 способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
ПК-30 способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;
ПК-32 способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

Студент должен знать:
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- требования нормативных правовых актов в области обеспечения информационной автоматизированных систем;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- критерии оценки эффективности средств защиты информационно-технологических ресурсов автоматизированной системы;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- содержание принципа комплексности при применении основных мер по защите информации в автоматизированных системах;
- основные методы управления информационной безопасностью;
- принципы формирования политики информационной безопасности в автоматизированных системах;

Студент должен уметь:

- планировать политику безопасности автоматизированных систем;
- оценивать эффективность применения средств защиты информации;
- эффективно использовать различные методы и средства защиты информации для автоматизированных систем;
- реализовывать политику информационной безопасности автоматизированных систем;
- применять средства обеспечения информационной безопасности;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- применять нормативные правовые документы при построении комплексных систем защиты информации;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по обеспечению комплекса мер защиты информации автоматизированных систем;
- разрабатывать и исследовать аналитические и компьютерные модели подсистем
- безопасности автоматизированных систем;
- администрировать подсистемы информационной безопасности автоматизированных систем;
- исследовать эффективность применяемых средств автоматизации;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;
- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- разрабатывать частные политики информационной безопасности автоматизированных систем;
- контролировать эффективность принятых мер по реализации частных политик
- информационной безопасности автоматизированных систем;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

Студент должен владеть:
- навыками работы с нормативными правовыми актами при комплексном подходе к обеспечению информационной безопасности автоматизированных систем;

- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- навыками разработки политики информационной безопасности автоматизированных систем;
- методами контроля эффективности принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
- навыками управления информационной безопасностью автоматизированных систем.