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.1.1.39 «Оценка информационной безопасности автоматизированных систем в защищенном исполнении»

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 – 9 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение основных стандартов, регламентирующих оценку информационной безопасности автоматизированных систем в защищенном исполнении.
Задачи изучения дисциплины:
– формирование у студентов целостного представления об оценке информационной безопасности автоматизированных систем в защищенном исполнении (АСЗИ);
– приобретение студентами необходимого объема знаний и практических навыков в области оценки средств информационной безопасности;
- развитие у студентов способности анализировать возможные вариант угроз и примерные портреты нарушителей безопасности системы,
- обучение студентов принципам разработки и внедрения АСЗИ,
- развитие у студентов принципов свободного оперирования методами создания и работы с АСЗИ,
- стимулирование у студентов эффективного применения действующих нормативных документов в процессе эксплуатации АСЗИ,
- развитие у студентов способности оценки уровня достаточности мер по обеспечению информационной безопасности при реализации задач АСЗИ.

2. Место дисциплины в структуре ООП ВО

Дисциплина "Оценка информационной безопасности автоматизированных систем в защищенном исполнении" относится к числу дисциплин специализации
9 «Создание автоматизированных систем в защищенном исполнении» профессионального цикла.

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

"*Правовое государство: история и современность*" – знать основы права и законодательства России, уметь использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; владеть навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

"*Основы информационной безопасности*" – знать сущность и понятие ИБ и характеристику ее составляющих, источники и классификацию угроз ИБ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности;

"*Разработка и эксплуатация защищенных автоматизированных*

систем" знать методы, способы, средства, последовательность и содержание этапов разработки подсистем безопасности АС, основные меры по защите информации в автоматизированных системах, криптографические методы, используемые для обеспечения ИБ в АС; владеть методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем, навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками анализа информационной инфраструктуры безопасности АС.

Знания и навыки, полученные при изучении дисциплины «*Оценка информационной безопасности автоматизированных систем в защищенном исполнении*», станут основой для подготовки выпускной квалификационной работы, выполнения заданий производственной практики, и будут актуальны в дальнейшей профессиональной деятельности.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- ПК-3 способность проводить анализ защищенности автоматизированных систем;
- ПК-17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
- ПСК-9.5 способность проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении.

Индекс **ПК-17**	**Формулировка:** **способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации**
Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительно)	**Знает**: - особенности рационального выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности, **Умеет**: - проводить верификацию элементов выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками проведения отбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.

Индекс **ПК-17**	**Формулировка:** **способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации**
Продвинутый (хорошо)	**Знает**: - особенности рационального выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, **Умеет**: - проводить верификацию элементов выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками проведения отбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы.
Высокий (отлично)	**Знает**: - особенности рационального выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: проводить верификацию элементов выбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - применять принципы разработки и внедрения АСЗИ. **Владеет**: - навыками проведения отбора методов и средств для реализации процессов создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - практикой применения принципов разработки и внедрения АСЗИ.

Индекс **ПК-3**	**Формулировка:** **способность проводить анализ защищенности автоматизированных систем**
Ступени уровней освоения компетенции	Отличительные признаки

Индекс **ПК-3**	**Формулировка:** **способность проводить анализ защищенности автоматизированных систем**
Пороговый (удовлетворительно)	**Знает**: - знает основные нормативно-правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности, **Умеет**: - проводить анализ основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками применения основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.
Продвинутый (хорошо)	**Знает**: - знает основные нормативно-правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, **Умеет**: - проводить анализ основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками применения основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы.

Индекс **ПК-3**	**Формулировка:** **способность проводить анализ защищенности автоматизированных систем**
Высокий (отлично)	**Знает**: - знает основные нормативно-правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: - проводить анализ основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - применять принципы разработки и внедрения АСЗИ. **Владеет**: - навыками применения основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - практикой применения принципов разработки и внедрения АСЗИ.

Индекс **ПСК-9.5**	**Формулировка:** **способность проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении**
Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительно)	**Знает**: - критерии анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности, **Умеет**: - проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками проведения анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.

Индекс ПСК-9.5	**Формулировка: способность проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении**
Продвинутый (хорошо)	**Знает**: - критерии анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, **Умеет**: - проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками проведения анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы.
Высокий (отлично)	**Знает**: - критерии анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: - проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - применять принципы разработки и внедрения АСЗИ. **Владеет**: - навыками проведения анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации АСЗИ; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности; - способностью анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы, - практикой применения принципов разработки и внедрения АСЗИ.