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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

С.3.2.2 «Комплексное обеспечение информационной безопасности автоматизированных систем»

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 – 6
часов в неделю – 5
всего часов – 216,
в том числе:
лекции – 36
лабораторные занятия – 54
самостоятельная работа – 126
курсовой проект – 9 семестр
экзамен – 9 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 научно-исследовательской и выпускной квалификационной работ.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-6 способность использовать нормативные правовые акты в своей профессиональной деятельности;

ПК-21 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-22 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;
ПК-33 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
ПК-34 способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы;
ПК-35 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
ПК-36 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы;
ПК-37 способность администрировать подсистему информационной безопасности автоматизированной системы;
ПК-38 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;
ПК-39 способность управлять информационной безопасностью автоматизированной системы;

Студент должен знать:

- требования нормативных правовых документов при построении комплексных систем защиты информации;
- принципы и методы проектирования системы управления информационной безопасностью автоматизированной системы;
- средства защиты информации и средства контроля защищенности автоматизированной системы;
- понятие, состав и содержание политики информационной безопасности организации, методы контроля эффективность ее реализации;
- содержание принципа комплексности при применении основных мер по защите информации в автоматизированных системах;
- информационно-технологические ресурсы автоматизированной системы и требования информационной безопасности при их применении;
- средства защиты информационно-технологических ресурсов автоматизированной системы;
- процедуру администрирования подсистему информационной безопасности автоматизированной системы;
- Принципы разработки частных политик информационной безопасности автоматизированной системы;
- методы управления информационной безопасностью автоматизированной системы

Студент должен уметь:

- применять нормативные правовые документы при построении комплексных систем защиты информации;
- выполнять задачи по проектированию системы управления информационной безопасностью автоматизированной системы;
- осуществлять выбор средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации;
- формировать политику информационной безопасности организации и контролировать эффективность ее реализации;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- обеспечивать эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
- эффективно применять средств защиты информационно-технологических ресурсов автоматизированной системы;
- администрировать подсистему информационной безопасности автоматизированной системы;
- выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;
- управлять информационной безопасностью автоматизированной системы.

Студент должен владеть:

- навыками работы с нормативными правовыми актами при построении комплексных систем защиты информации;
- навыком участия в проектировании системы управления информационной безопасностью автоматизированной системы;
- навыком участия в выборе средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации;
- навыком формирования политики информационной безопасности организации и контроля эффективность ее реализации;
- навыками формирования комплекса мер для обеспечения информационной безопасности автоматизированных систем;
- навыком обеспечения эффективного применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

- навыком эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы;
- навыком администрирования подсистемы информационной безопасности автоматизированной системы;
- навыком выполнения частных политик информационной безопасности автоматизированной системы и осуществления мониторинга безопасности автоматизированной системы;
- навыком управления информационной безопасностью автоматизированной системы.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ модуля	№ недели	№ темы	Наименование темы	Часы/ Из них в интерактивной форме				
				Всего	Лекции	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
8 семестр								
1	1	1	Сущность и задачи комплексной защиты информации.	14	2	2		10
1	2	2	Принципы организации и этапы разработки КСЗИ.	30	6/2	10/4		14
1	5	3	Определение и нормативное закрепление состава защищаемой информации.	28	4/2	6		18
1	7	4	Каналы и методы дестабилизирующего воздействия на информацию.	28	4/2	6		18
2	9	5	Разработка модели комплексной системы защиты информации.	30	6/4	8/2		16
2	12	6	Определение компонентов комплексной системы защиты информации	36	6/4	10/8		20
2	15	7	Назначение, структура и содержание управления комплексной системой защиты информации	26	4/2	6/2		16
2	17	8	Оценка эффективности комплексной системы защиты информации.	24	4/2	6/2		14
Всего				216/36	36/18	54/18		126

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	**2**	**1**	**Сущность и задачи комплексной защиты информации.** Понятийный аппарат в области обеспечения безопасности информации. Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации. Цели, задачи и принципы построения комплексной системы защиты информации.	2,3,4,5,22
2	**6**	**2,3,4**	**Принципы организации и этапы разработки КСЗИ.** Методологические основы организации комплексной системой защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Требования, предъявляемые к комплексной системе защиты информации. Требования к организационной и технической составляющим комплексной системы защиты информации. Требования по безопасности, предъявляемые к изделиям ИТ. Этапы разработки комплексной системы защиты информации. Факторы, влияющие на организацию комплексной системы защиты информации.	2,3,4,7,12,22
3	**4**	**5,6**	**Определение и нормативное закрепление состава защищаемой информации.** Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение объектов защиты. Значение носителей защищаемой информации как объектов защиты.	3,4,7,8,11,22
4	**4**	**7,8**	**Каналы и методы дестабилизирующего воздействия на информацию**. Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС. Подходы к оценке ущерба от нарушений ИБ. Задачи комплексной системы защиты информации по выявлению угроз и каналов утечки информации.	2,3,4,9,11,22
5	**6**	**9,10,11**	**Разработка модели комплексной системы защиты информации.** Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности и их анализ.	2,3,4,6,22

			Классификация формальных моделей безопасности. Модели обеспечения конфиденциальности. Модели обеспечения целостности. Субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: пример. Описание объекта защиты. Декомпозиция АС на субъекты и объекты. Модель безопасности: неформальное описание. Декомпозиция системы защиты информации. Противостояние угрозам. Реализация системы защиты информации субъекта АС субъектно-объектной модели.	
6	**6**	**12,13,14**	**Определение компонентов комплексной системы защиты информации.** Технологическое построение комплексной системы защиты информации. Формулирование требований к системе защиты информации. Выбор механизмов и средств защиты информации. Определение важности параметров средств защиты информации. Оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС.	2,3,4,9,10,11,22
7	**4**	**15,16**	**Назначение, структура и содержание управления комплексной системой защиты информации.** Понятие, сущность и цели управления комплексной системой защиты информации. Принципы управления комплексной системой защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системой защиты информации. Структура и содержание общей технологии управления комплексной системой защиты информации. Принципы и методы планирования функционирования комплексной системы защиты информации. Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системе защиты информации. Анализ и использование результатов проведения контрольных мероприятий.	1,2,4,5,11,22
8	**4**	**17,18**	**Оценка эффективности комплексной системы защиты информации.** Общая характеристика подходов к оценке эффективности комплексной системы защиты информации. Методы и модели оценки эффективности КСЗИ. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса	1,2,4,5,11,22

6. Содержание коллоквиумов

Коллоквиумы учебным планом не предусмотрены.

7. Перечень практических занятий

Практические занятия учебным планом не предусмотрены.

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	4	3
1	2	Выявление факторов, влияющих на организацию комплексной системы защиты информации	2,3,4,5,22
2	10	Разработка политики информационной безопасности	2,3,4,7,12,22
3	6	Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих конфиденциальную информацию предприятия, внесение в него изменений и дополнений. Методика выявления состава носителей защищаемой информации.	3,4,7,8,11,22
4	6	Разработка модели угроз и модели нарушителя. Методика выявления нарушителей, тактики их действий и состава интересующей их информации.	2,3,4,9,11,22
5	8	Формальное построение модели защиты	2,3,4,6,22
6	10	Проектирование системы зашиты информации для существующей АС	2,3,4,9,10,11,22
7	6	Планирование процесса функционирования комплексной системы защиты информации	1,2,4,5,11,22
8	6	Модели оценки эффективности комплексной системы защиты информации	1,2,4,5,11,22

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
2	10	Методология защиты информации. Современный подход	1-22
3	14	Подходы к проектированию систем защиты информации	1-22
3	18	Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав средств обеспечения, подлежащих защите	1-22
4	18	Обеспечение безопасности информации в непредвиденных ситуациях. Реагирование на инциденты информационной безопасности. Резервирование информации и отказоустойчивость	1-22
5	16	Оптимальное построение системы защиты информации.	1-22
6	20	Формализация модели безопасности. Процедура	1-22

		создания пары субъект—объект, наделение их атрибутами безопасности. Осуществление доступа субъекта к объекту. Взаимодействие с внешними сетями. Удаление субъекта—объекта.	
7	16	Аудит информационной безопасности	1-22
8	14	Экономический подход к оценке эффективности комплексной системы защиты информации.	1-22

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
9 семестр			
1-4	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), экзамен
5-8	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Экзамен, курсовой проект

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Задание по курсовому проектированию включает в себя выполнение исследовательской и проектной части.

12.1. Темы исследовательской части курсового проекта

1. Цели и задачи построения КСЗИ
2. Разработка политики безопасности предприятия
3. Система управления информационной безопасностью предприятия
4. Этапы разработки КСЗИ
5. Исследование факторов, влияющих на организацию КСЗИ
6. Определение объектов защиты на предприятии
7. Методика определения состава защищаемой информации
8. Подходы к оценке ущерба от нарушений ИБ
9. Кадровое обеспечение функционирования КСЗИ
10. Материально-техническое обеспечение КСЗИ
11. Нормативно-методическое обеспечение КСЗИ
12. Планирование функционирования КСЗИ

13. Оценка эффективности КСЗИ
14. Определение источников дестабилизирующего воздействия на информацию
15. Внедрение КСЗИ в организации
16. Аттестация объекта информатизации
17. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы
18. Методы и средства обеспечения информационной безопасности АС
19. Угрозы ИБ АС
20. Методика проведения аудита информационной безопасности на предприятии
21. Программные средства для проведения аудита информационной безопасности на предприятии
22. Управление КСЗИ в условиях чрезвычайных ситуаций
23. Контроль функционирования КСЗИ
24. Особенности работы с персоналом, владеющим конфиденциальной информацией
25. Принципы построения КСЗИ
26. Этапы проектирования КСИБ
27. Инженерно-техническая защита АС предприятия

12.2. Задание практической части курсового проекта содержит разработку системы обеспечения информационной безопасности информационной системы персональных данных.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Формирование компетенций по дисциплине производится на занятиях по лабораторным работам и лекционных занятиях, в рамках выполнения самостоятельной работы; закрепление достигается при проведении промежуточной аттестации и сдаче экзамена.

Перечень компетенций с указанием этапов их формирования и критериев оценивания

№ п/п	Наименование компетенции	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5

1.	ПК-6: способностью использовать нормативные правовые акты в своей профессиональной деятельности	Знает: требования нормативных правовых документов при построении комплексных систем защиты информации	Лекции Самостоятельная работа	Экзамен
		Умеет: применять нормативные правовые документы при построении комплексных систем защиты информации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыками работы с нормативными правовыми актами при построении комплексных систем защиты информации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
2.	ПК-21: способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знает: требования нормативных правовых документов при построении комплексных систем защиты информации	Лекции Самостоятельная работа	Экзамен
		Умеет: применять нормативные правовые документы при построении комплексных систем защиты информации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыками работы с нормативными правовыми актами при построении комплексных систем защиты информации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
3.	ПК-22: способностью участвовать в проектировании средств защиты информации и средств контроля защищенности	Знает: средства защиты информации и средства контроля защищенности автоматизированной системы	Лекции Самостоятельная работа	Экзамен
		Умеет:	Лабораторные	Текущий

	автоматизированной системы	осуществлять выбор средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации	работы Курсовой проект Самостоятельная работа	контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком участия в выборе средств защиты информации и средств контроля защищенности автоматизированной системы при проектировании комплексных систем защиты информации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
4.	ПК-33: способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знает: понятие, состав и содержание политики информационной безопасности организации, методы контроля эффективность ее реализации	Лекции Самостоятельная работа	Экзамен
		Умеет: формировать политику информационной безопасности организации и контролировать эффективность ее реализации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком формирования политики информационной безопасности организации и контроля эффективность ее реализации	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
5.	ПК-34: способностью формировать комплекс мер	Знает: содержание принципа комплексности при применении основных	Лекции Самостоятельная работа	Экзамен

	(правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы	мер по защите информации в автоматизированных системах		
		Умеет: определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыками формирования комплекса мер для обеспечения информационной безопасности автоматизированных систем	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
6.	ПК-35: способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Знает: информационно-технологические ресурсы автоматизированной системы и требования информационной безопасности при их применении	Лекции Самостоятельная работа	Экзамен
		Умеет: обеспечивать эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком обеспечения эффективного применение информационно-	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового

		технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		проекта, самостоятельной работы
7.	ПК-36: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы	Знает: средства защиты информационно-технологических ресурсов автоматизированной системы	Лекции Самостоятельная работа	Экзамен
		Умеет: эффективно применять средств защиты информационно-технологических ресурсов автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
8.	ПК-37: способностью администрировать подсистему информационной безопасности автоматизированной системы	Знает: процедуру администрирования подсистему информационной безопасности автоматизированной системы	Лекции Самостоятельная работа	Экзамен
		Умеет: администрировать подсистему информационной безопасности автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком администрирования подсистемы	Лабораторные работы Курсовой проект	Текущий контроль выполнения

		информационной безопасности автоматизированной системы	Самостоятельная работа	лабораторных работ, курсового проекта, самостоятельной работы
9.	ПК-38: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Знает: Принципы разработки частных политик информационной безопасности автоматизированной системы	Лекции Самостоятельная работа	Экзамен
		Умеет: выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной работы
		Владеет: навыком выполнения частных политик информационной безопасности автоматизированной системы и осуществления мониторинга безопасности автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы
10.	ПК-39: способностью управлять информационной безопасностью автоматизированной системы	Знает: методы управления информационной безопасностью автоматизированной системы	Лекции Самостоятельная работа	Экзамен
		Умеет: управлять информационной безопасностью автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта работы, самостоятельной

				работы
		Владеет: Навыком управления информационной безопасностью автоматизированной системы	Лабораторные работы Курсовой проект Самостоятельная работа	Текущий контроль выполнения лабораторных работ, курсового проекта, самостоятельной работы

Уровни освоения компетенций

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на достаточном уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на достаточном уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на достаточном уровне освоения
Продвинутый (хорошо)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на хорошем уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на достаточном хорошем уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на хорошем уровне освоения
Высокий (отлично)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на высоком уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на высоком уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на высоком уровне освоения

Уровень освоения обучающимися дисциплины оценивается по результатам приема экзамена.

Результаты экзамена оцениваются «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

- оценки "отлично" заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на высоком уровне освоения, усвоивший взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявивший творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценки "хорошо" заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, продемонстрировавший умения и навыки в рамках формируемых компетенций на хорошем уровне освоения, способный к

самостоятельному выполнению заданий в ходе дальнейшей учебной работы и профессиональной деятельности;

- оценки "удовлетворительно" заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, освоившийся с выполнением заданий, предусмотренных программой, допустивший неточности в ответе на экзамене;

- оценки "неудовлетворительно" заслуживает студент, обнаруживший пробелы в знании основного учебно-программного материала, допустивший существенные ошибки в ответах на экзамене, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения.

Вопросы для экзамена

1. Цели и задачи защиты информации в автоматизированных системах.
2. Цели, задачи и принципы построения комплексной системы защиты информации.
3. Политика безопасности и регламент безопасности предприятия.
4. Система управления информационной безопасностью предприятия.
5. Требования, предъявляемые к комплексной системе защиты информации.
6. Этапы разработки комплексной системы защиты информации. Факторы, влияющие на организацию комплексной системы защиты информации.
7. Классификация информации по видам тайны и степеням конфиденциальности.
8. Нормативно-правовые аспекты определения состава защищаемой информации.
9. Определение объектов защиты.
10. Факторы, создающие угрозу информационной безопасности.
11. Угрозы безопасности информации.
12. Модели нарушителей безопасности АС.
13. Оценка ущерба от нарушений ИБ.
14. Задачи комплексной системы защиты информации по выявлению угроз и каналов утечки информации.
15. Описание архитектуры АС, системы защиты информации и политики безопасности.
16. Характеристика задач моделирования КСЗИ.
17. Понятие, сущность и цели управления комплексной системой защиты информации.
18. Принципы управления комплексной системой защиты информации. Структура процессов управления.
19. Оценка эффективности комплексной системы защиты информации.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВПО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами решения ситуационных задач, дискуссий.

Общее количество занятий, проводимых в интерактивных формах, не менее 36 часов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Аверченков В.И. Системы организационного управления [Электронный ресурс]: учебное пособие/ Аверченков В.И., Ерохин В.В.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 208 с.— Режим доступа: http://www.iprbookshop.ru/7013.— ЭБС «IPRbooks», по паролю
2. Карпов В.В. Технология построения защищенных автоматизированных систем [Электронный ресурс]: учебное пособие/ Карпов В.В., Мельник В.А.— Электрон. текстовые данные.— М.: Российский новый университет, 2009.— 232 с.— Режим доступа: http://www.iprbookshop.ru/21326.— ЭБС «IPRbooks», по паролю
3. Пластун, И. Л. Технология построения защищенных автоматизированных систем и сетей : учеб. пособие для студ. спец. 075500, 220400 / И. Л. Пластун; М-во образования и науки Рос. Федерации, Саратовский гос. техн. ун-т. - Саратов : СГТУ, 2010. - 96 с. 40 экз
4. Куприянов, А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. 22 экз.

Дополнительные издания

5. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/12048.— ЭБС «IPRbooks», по паролю

6. Грушо, А. А. Теоретические основы компьютерной безопасности : учеб. пособие / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : ИЦ "Академия", 2009. - 272 с. 10 экз
7. Девянин, П. Н. Модели безопасности компьютерных систем : учеб. пособие для вузов / П. Н. Девянин. - М. : ИЦ "Академия", 2005. - 144 с. 12 экз
8. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). - Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf.
9. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - М. : ИЦ "Академия", 2006. - 240 с. 19 экз
10. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - 4-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. 18 экз
11.Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю
12.Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

Периодические издания

13. Вестник СГТУ (http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan)
14. Инновационная деятельность (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/)
15. Журнал «Инновации + Паблисити» (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/)

Интернет-ресурсы

16. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
17. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. URL:http://www.securitylab.ru/ (дата обращения: 1.06.2015).
18.Информационная безопасность регионов (http://www.seun.ru/content/nauka /5/1/index.php).

19. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
20. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
21. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

22. Весь учебно-методический материал размещен в электронной форме в ИОС специальности ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А.

16. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий используется типовая лекционная аудитория со стандартным мультимедийным оснащением:

- персональный компьютер (в конфигурации не хуже: процессор Intel Pentium или AMD 2 ГГц, 2 ОЗУ Гбайта, 320 Гбайт НЖМД);
- проектор (разрешение не менее 1024x768);
- экран для проектора.

Для проведения лабораторных работ и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория кафедры ИБС, оснащенная вычислительной техникой: ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт, с подключением к локальной сети СГТУ имени Гагарина Ю.А. и доступом к сети Интернет.

При проведении лабораторных работ в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционная система: Windows XP/7.
2. ГАРАНТ аэро (Клиент) Текущий Пользователь
3. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.