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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА
по дисциплине

Б.1.1.34 «Создание автоматизированных систем в защищенном исполнении»

направления подготовки
10.03.01 «Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 3
часов в неделю – 3
академических часов – 108
в том числе:
лекции – 16
практические занятия – 32
самостоятельная работа – 60
зачет – 7 семестр
курсовой проект – 7 семестр

1. Цели и задачи дисциплины

Дисциплина «Создание автоматизированных систем в защищенном исполнении» имеет **целью** изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения автоматизированных систем на предприятиях различных отраслей промышленности с учетом требований по обеспечению информационной безопасности.

Задачами дисциплины являются:

- формирование у обучаемых целостного представления о содержании и организации процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.
- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации методов, процессов, инструментов и средств защиты автоматизированных систем;

2. Место дисциплины в структуре ООП ВО

Курс «Создание автоматизированных систем в защищенном исполнении»относится к дисциплинам вариативной части профессионального цикла учебного плана и читается студентам в первом семестре последнего (четвертого) года обучения. Данная дисциплина опирается на знания, полученные студентами ранеепри изучении курсовпрофессионального цикла, таких как «Безопасность операционных систем», «Безопасность систем баз данных», «Основы информационной безопасности», «Техническая защита информации», «Организация ЭВМ и вычислительных систем», «Криптографические методы защиты информации», «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности»

3. Требования к результатам освоения дисциплины

В результате изучения дисциплины студент должен обладать следующими компетенциями:

- **ПК-5** - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- **ПК-7** - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- **ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

- **ПСК-4.1** - способность применять нормативные правовые акты и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении.

Студент должен знать:
- основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении;
- общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;

Студент должен уметь:
- разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
- формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов;
- осуществлять подбор и комплексирование средств защиты для автоматизированных систем в защищенном исполнении;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
- контролировать эффективность проектирования, разработки и внедрения автоматизированных систем;

Студент должен владеть:
- навыками разработки моделей угроз и моделей нарушителей;
- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- навыками участия в экспертизе состояния защищенности информации на объекте защиты.

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

№ модуля	№ недели	№ темы	Наименование темы	Часы / Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лаб. занятия	Практ. занятия	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1-2	1	Общий порядок проектированияАС	10	2			2	6
1	3-6	2	Проектирование АС в защищенном исполнении	27/3	4/3			2	21
2	7-8	3	Модель угроз	8/1	2/1			-	6
2	9-10	4	Модель нарушителя	8/1	2/1			-	6
3	11-14	5	Создание систем защиты ПДн	30/2	4/2			16	10
3	15-18	6	Основные категории средств защиты информации в АС	25/3	4/3			16	5
Всего				108/10	18/10				54

№ модуля	№ недели	№ темы	Наименование темы	Часы / Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лаб. занятия	Практ. занятия	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1-4	1	Общий порядок проектированияАС	24	4			8	12
1	5-8	2	Проектирование АС в защищенном исполнении	28/3	4/3			8	16
2	9-10	3	Модель угроз, модель нарушителя	14/1	2/1			4	8
2	11-12	4	Создание систем защиты ПДн	14/1	2/1			4	8
2	13-16	5	Основные категории средств	28/2	4/2			8	16

			защиты информации в АС						
Всего				108/10	16/10			32/12	60

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	**Общий порядок проектирования АС.** Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения.	[1,2,3,5,10, 12,13]
1	2	2	**Понятие АС**. Классификация АС. Жизненный цикл АС. **Стандарты** (ГОСТ), регламентирующие порядок проектирования АС.	[1,2,3,5,10, 12,13]
2	2	3	**Проектирование АС в защищенном исполнении.** Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Общий порядок проектирования систем в защищенном исполнении.	[1,2,3,5,10, 12,13]
2	2	4	**Стандарты** (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении. Руководящие документы Гостехкомиссии России (ФСТЭК России).	[1,2,3,5,10, 12,13]
3	2	5	**Модели угроз.** Понятие модели угроз. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Практические подходы к разработке моделей угроз. **Модели нарушителя.** Понятие модели нарушителя. Документы ФСТЭК России, регламентирующие порядок разработки моделей нарушителя в автоматизированных системах. Практические подходы к разработке моделей нарушителя.	[2,6,8,9,10,12 , 13] [2,6,8,9,10, 12,13]

4	2	6	**Создание систем защиты персональных данных.** Понятие персональных данных. Понятие ИСПДн. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России). Требования к ИСПДн. **Основные категории средств защиты ИСПДн.** Рекомендации по выбору средств защиты. **Обезличивание персональных данных**.	[2,8,9,10,11, 12,13]
5	2	7	**Основные категории средств защиты информации в АС**	[2,8,9,10,11, 12,13]
5	2	8	**Сертификация средств защиты ИСПДн**. Особенности лицензирования соответствующих видов деятельности. Аттестация ИСПДн.	[2,3,4,6,7,8, 10,12,13]

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
Учебным планом не предусмотрены				

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	2	1	ГОСТ 34.003.90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения	[10,11,12]
	2	2	ГОСТ 34.201 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем	[10,11,12]
	2	3	ГОСТ 34.601 Информационная технология. Комплекс стандартов на	[10,11,12]

			автоматизированные системы. Автоматизированные системы. Стадии создания	
			ГОСТ 34.602 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы	[10,11,12]
	2	4	ГОСТ 34.603 Информационная технология. Виды испытаний автоматизированных систем	[10,11,12]
			ГОСТ 16504 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения	[10,11,12]
2	2	5	ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения	[10,11,12]
			ГОСТ Р 50922 Защита информации. Основные термины и определения	[10,11,12]
			ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения	[10,11,12]
	2	6	ГОСТ Р 54869 Проектный менеджмент. Требования к управлению проектом	[10,11,12]
			ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности	[10,11,12]
			ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель	[10,11,12]
			ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности	[10,11,12]
			ГОСТ Р ИСО/МЭК 15408-	[10,11,12]

			3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности	
			ГОСТ Р ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий	[10,11,12]
	2	7	ГОСТ Р ИСО/МЭК 21827 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса	[10,11,12]
			ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности	[10,11,12]
	2	8	ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности	[10,11,12]
			ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем	[10,11,12]
3	2	9	Методика определения угроз безопасности информации в информационных системах	[10,11,12]
	2	10	Модель нарушителя безопасности персональных данных при их обработке в информационной системе	[10,11,12]
4	4	11-12	Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»	[10,11,12]
5	2		Практическая реализация алгоритма VS-AES.	[2,6,13]
	2		Практическая реализация алгоритма RSA	[2,6,13]
	2		Практическая реализация алгоритма Диффи – Хэллмана	[2,6,13]
	2		Практическая реализация алгоритма Эль - Гамаля.	[2,6,13]

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	3	4
Учебным планом не предусмотрены			

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации. Большинство средств зашиты информации базируется на использовании криптографических шифров и процедур шифрования-дешифрования.

При выполнении предлагаемых заданий студент должен ознакомиться с основными методами криптографической защиты и получить практические навыки криптографических преобразований информации.

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Вопросы для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
1	12	Порядок создания автоматизированных систем автоматизированная система	[10,11,12]
2	2	ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.	[10,11,12]
	2	ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.	[10,11,12]
	2	ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.	[10,11,12]
	2	ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.	[10,11,12]
	2	ГОСТ Р ИСО/МЭК 15408 — «Общие критерии	[10,11,12]

		оценки безопасности информационных технологий».	
	2	ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.	[10,11,12]
	2	ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005	[10,11,12]
	2	ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.	[10,11,12]
3	3	Модели угроз информационной безопасности	[9,10,13]
	3	Модель нарушителя информационной безопасности	[9,10,13]
	2	Практические подходы к разработке моделей нарушителя.	[9,10,13]
4	2	Персональные данные. Особенности хранения и передачи	[5,10,11,12]
	2	Понятие и требования к ИСПДн	[10,11,13]
	2	Понятие персональных данных. Понятие ИСПДн.	[10,11,13]
	2	Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).	[10,11,13]
5	8	Основные категории средств защиты информации	
5	8	Сертификация средств защиты информации	[10,13]

10. Расчетно-графическая работа

Учебным планом не предусмотрена.

11. Курсовая работа

Учебным планом не предусмотрена

12. Курсовой проект

Целью выполнения курсового проекта является закрепление и углубление теоретических знаний, полученных в процессе обучения, их систематизация и

развитие, а также получение практических навыков в области исследования систем защиты информации на предприятии.

Курсовой проект должен содержать введение, теоретическую и практическую части, заключение и список литературы. Во введении кратко освещается состояние проблемы и ситуация, в которой она решается, отмечаются основные цели и определяются задачи для достижения поставленных целей, определяется объект и предметная область исследования. В теоретической части проекта рассматриваются основные теоретические положения, раскрывающие суть темы курсовой работы. Практическая часть проекта включает: практическую реализацию теоретических положений на примере предприятия (организации), с проведением экономического обоснования разработанных предложений (проекта). В заключении подводятся итоги проекта, делаются выводы на основе проведенного исследования, намечаются возможные пути и рекомендации для дальнейшего совершенствования рассматриваемой проблемы.

Перечень тем курсовых проектов

- Методика классификации угроз безопасности информации в организации.
- Методика оценки угроз безопасности информации в информационной системе организации от несанкционированного доступа.
- Методика оценки угроз безопасности информации от утечки по техническим каналам.
- Методика определения перечня сведений, подлежащих защите, в организации.
- Методика определения перечня носителей сведений, подлежащих защите в организации.
- Организация инженерно-технической охраны объектов.
- Организация инженерно-технической защиты объектов от утечки информации по техническим каналам.
- Организация защиты информации в локальной сети организации от несанкционированного доступа.
- Методика выбора программно-аппаратных средств защиты информации в ЛВС организации от несанкционированного доступа.
- Методика выбора программно-аппаратных средств защиты информации в интранет-сети организации от несанкционированного доступа.
- Методика выбора СКУД для организации пропускного режима в организации.
- Методика построения комплексной системы защиты информации в организации.
- Анализ и оценка рисков безопасности информации в организации от утечки по техническим каналам.
- Анализ и оценка рисков безопасности информации в ЛВС организации от несанкционированного доступа.
- Анализ и оценка рисков безопасности информации в интранет-сети организации от несанкционированного доступа.
- Методика разработки «Положения о коммерческой тайне организации».

- Методика разработки «Политики безопасности информации в информационной системе организации».
- Методика проведения аудита безопасности информации в организации.
- Методика построения модели угроз безопасности информации в организации от несанкционированного доступа.
- Методика построения модели угроз безопасности информации в организации утечки по техническим каналам.
- Методика организации режима коммерческой тайны в организации.
- Методика организации и проведения конфиденциальных переговоров в организации.
- выявления состава носителей защищаемой информации.
- Организация кадровой работы с персоналом по вопросам информационной.
- Методика выбора структуры комплексной системы обеспечения информационной безопасности.
- Методика оценки эффективности комплексной системы обеспечения информационной безопасности в организации.

Студент защищает курсовой проект перед комиссией. Защита курсового проекта включает краткий доклад студента (не более 5 минут), и ответы на вопросы по существу работы.

Результаты защиты курсового проекта оцениваются «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценки «отлично» заслуживает студент, полностью выполнивший задание, показавшему глубокое и всестороннее знание теоретической части, грамотно оформившему техническую документацию.

Оценки «хорошо» заслуживает студент, полностью выполнивший задание, показавшему знание теоретической части.

Оценки «удовлетворительно» заслуживает студент полностью выполнивший задание, однако, при защите обнаруживший пробелы в знаниях теоретической части.

Оценка «неудовлетворительно» выставляется студенту, не выполнившему задание по курсовому проекту в полном объеме, не освоившему умения и навыки в рамках формируемых компетенций на достаточном уровне освоения.

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

Профессиональные компетенции, знания, навыки и умения оцениваются в соответствии с требованиями ФГОС ВО по направлению10.03.01.

В процессе освоения дисциплины осуществляется формирование следующих компетенций:

- **ПК-5** - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
- **ПК-7** - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений,
- **ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов,
- **ПСК-4.1** - способность применять нормативные правовые акты и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении

Составляющие компетенций

- **ПК-5** - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3
Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • порядок проведения аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем	Лекции Самостоятельная работа	Тестирование Зачет

Умеет: • определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;	Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование Доклады Курсовая работа
Владеет: • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; • навыками участия в экспертизе состояния защищенности информации на объекте защиты.	Лекции Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

- **ПК-7** - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений,

Части компонентов	**Технологии формирования**	**Средства и технологии оценки**
1	**2**	**3**
Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем	Лекции Самостоятельная работа	Тестирование Зачет

Умеет: • контролировать эффективность проектирования, разработки и внедрения автоматизированных систем;	Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование Доклады Курсовая работа
Владеет: • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; • навыками участия в экспертизе состояния защищенности информации на объекте защиты.	Лекции Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

- **ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов,

Части компонентов	**Технологии формирования**	**Средства и технологии оценки**
1	**2**	**3**
Знает: основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении;	Лекции Самостоятельная работа	Тестирование Зачет
Умеет: составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;	Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование Доклады Курсовая работа

Владеет: навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;	Лекции Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

- **ПСК-4.1** - способность применять нормативные правовые акты и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении

Части компонентов	**Технологии формирования**	**Средства и технологии оценки**
1	**2**	**3**
Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем;	Лекции Самостоятельная работа	Тестирование Зачет
Умеет: • формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов; • определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;	Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование Доклады Курсовая работа

Владеет: навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;	Лекции Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

Уровни освоения компетенций

- **ПК-5** - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Ступени уровней освоения компетенции	**Отличительные признаки**
1	**2**
Пороговый (удовлетворительный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем Умеет: • определять комплекс мер для обеспечения информационной безопасности автоматизированных систем;
Продвинутый (хороший)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем Умеет: • определять комплекс мер для обеспечения информационной безопасности автоматизированных систем; Владеет: • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных

	систем;
Высокий (отличный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • порядок проведения аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем Умеет: • определять комплекс мер для обеспечения информационной безопасности автоматизированных систем, с учетом их специфики; Владеет: • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; • навыками участия в экспертизе состояния защищенности информации на объекте защиты.

- **ПК-7** - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений,

Ступени уровней освоения компетенции	**Отличительные признаки**
1	**2**
Пороговый (удовлетворительный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем

Продвинутый (хороший)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем Умеет: • контролировать эффективность проектирования, разработки и внедрения автоматизированных систем;
Высокий (отличный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем Умеет: • контролировать эффективность проектирования, разработки и внедрения автоматизированных систем; Владеет: • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; • навыками участия в экспертизе состояния защищенности информации на объекте защиты. •

- **ПК-8** - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов,

Ступени уровней освоения компетенции	**Отличительные признаки**
1	**2**
Пороговый (удовлетворительный)	Знает: основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; Умеет: составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;

Продвинутый (хороший)	Знает: основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; Умеет: составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; Владеет: навыками выбора критериев эффективности функционирования защищенных автоматизированных информационных систем;
Высокий (отличный)	Знает: основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; Умеет: составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; Владеет: навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;

- **ПСК-4.1** - способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем

Ступени уровней освоения компетенции	**Отличительные признаки**
1	**2**
Пороговый (удовлетворительный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем; • программно-аппаратные средства защиты информации Умеет: • формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов; • определять необходимый уровень защиты

	информационной системы; .
Продвинутый (хороший)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем; • программно-аппаратные средства защиты информации Умеет: • формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов; • определять необходимый уровень защиты информационной системы; • проектировать подсистемы безопасности автоматизированных систем Владеет: • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; • навыками практического применения программно-аппаратные средства защиты информации
Высокий (отличный)	Знает: • основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении; • общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем; • программно-аппаратные средства защиты информации Умеет: • формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов; • определять необходимый уровень защиты информационной системы; • проектировать подсистемы безопасности автоматизированных систем • выбирать оптимальную конфигурацию подсистемы информационной безопасности автоматизированной системы

	Владеет: • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; • навыками выбора и обоснования комплекта программно-технических средств информационной защиты автоматизированной системы • навыками практического применения программно-аппаратные средства защиты информации

Формирование профессиональных компетенций по дисциплине производится на лабораторных и лекционных занятиях (50%), при выполнении курсовогопроекта (20 %), а также в процессе самостоятельной работы (10%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче зачета (10%).

При выставлении экзаменационных оценок преподаватель руководствуется следующим:

- оценки «зачтено» 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, знакомый с основной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на достаточном уровне освоения;

- оценка «не зачтено» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившего принципиальные ошибки в выполнении предусмотренных программой заданий, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для зачета

1. Основные понятия и определения. Понятие автоматизированной системы.
2. Особенности автоматизированных систем в защищенном исполнении.
3. Основные виды АС в защищенном исполнении.
4. Общий порядок проектирования систем в защищенном исполнении. Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении.
5. Руководящие документы Гостехкомиссии России (ФСТЭК России).
6. Понятие модели угроз. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Практические подходы к разработке моделей угроз.

7. Понятие модели нарушителя. Документы ФСТЭК России, регламентирующие порядок разработки моделей нарушителя в автоматизированных системах.
8. Практические подходы к разработке моделей нарушителя.
9. Понятие персональных данных. Понятие ИСПДн.
10. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).
11. Требования к ИСПДн. Классификация АС. Обезличивание персональных данных.
12. Типовые модели угроз и модели нарушителя.
13. Практические рекомендации по разработке моделей угроз и моделей нарушителя.
14. Рекомендации по выбору средств защиты. Сертификация средств защиты ИСПДн.
15. Особенности лицензирования соответствующих видов деятельности. Аттестация ИСПДн.
16. Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса.

Вопросы для экзамена

Учебным планом не предусмотрен.

Тестовые задания по дисциплине

Вопрос 1. Какую цель преследуют хакеры – дилетанты:
1) добиться доступа к системе, чтобы выяснить ее назначение;
2) модифицировать или стереть данные, а также оставить преднамеренный след, например, в виде непристойной записки;
3) совершенствуют систему безопасности предприятия

Вопрос 2 Кого обычно относят к категории хакеров-профессионалов:
1) лиц, стремящихся получить информацию в целях промышленного шпионажа;
2) «белые воротнички» работающие на разные компании, чтобы усовершенствовать их систему безопасности;
3) группировки отдельных лиц, стремящихся к наживе.

Вопрос 3. Что относится к техническим средствам НСД:
1) телефонные автонабиратели;
2) логические бомбы;
3) экранный имитатор;
4) получение паролей.

Вопрос 4. Что относится к программным средствам НСД:
1) антивирусные программы;

2) троянский конь;
3) протоколы связи;
4) получение паролей.

Вопрос 5. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?
1) получить, изменить, а затем передать ее конкурентам;
2) размножить или уничтожить ее;
3) получить, изменить или уничтожить;
4) изменить и уничтожить ее;
5) изменить, повредить или ее уничтожить.

Вопрос 6. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
1) любая информация;
2) только открытая информация;
3) запатентованная информация;
4) закрываемая собственником информация;
5) коммерческая тайна.

Вопрос 7. Кто может быть владельцем защищаемой информации?
1) только государство и его структуры;
2) предприятия акционерные общества, фирмы;
3) общественные организации;
4) только вышеперечисленные;
5) кто угодно.

Вопрос 8. Какие сведения на территории РФ могут составлять коммерческую тайну?
1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;
3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
4) другие;
5) любые.

Вопрос 9. Какой самый прямой и эффективный способ склонения к сотрудничеству?
1) психическое давление;
2) подкуп;
3) преследование;
4) шантаж;
5) угрозы.

Вопрос 10. Завершающим этапом любого сбора конфиденциальной информации является
1) копирование;
2) подделка;
3) аналитическая обработка;
4) фотографирование;
5) наблюдение.

Вопрос 11Причины связанные с информационным обменом приносящие наибольшие убытки?
1) остановка или выход из строя информационных систем;
2) потери информации;
3) неискренность;
4) проникновение в информационную систему;
5) перехват информации.

Вопрос 12. Какие цели преследуются при активном вторжении в линии связи?
1) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
3) инициализация ложных соединений;
4) варианты 1 и 2;
5) варианты 2 и 3.

Вопрос 13. Что определяет модель нарушителя?
1) категории лиц, в числе которых может оказаться нарушитель;
2) возможные цели нарушителя и их градации по степени важности и опасности;
3) предположения о его квалификации и оценка его технической вооруженности;
4) ограничения и предположения о характере его действий;
5) все выше перечисленные.

Вопрос 14. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.
1) ознакомление с информационной системой или вычислительной сетью;
2) похитить программу или иную информацию;
3) оставить записку, выполнить, уничтожить или изменить программу;
4) вариант 2 и 3;
5) вариант 1, 2 и 3.

Вопрос 15. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?
1) скрытие;

2) дезинформация;
3) дробление;
4) кодирование;
5) шифрование.

Вопрос 16. Что в себя включают морально-нравственные методы защиты информации?
1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
2) контроль работы сотрудников, допущенных к работе с секретной информацией;
3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
4) вариант ответа 1 и 3;
5) вариант ответа 1, 2 и 3.

Вопрос 17. Что включают в себя технические мероприятия по защите информации?
1) поиск и уничтожение технических средств разведки;
2) кодирование информации или передаваемого сигнала;
3) подавление технических средств постановкой помехи;
4) применение детекторов лжи;
5) все вышеперечисленное.

Вопрос 18. Какие основные направления в защите персональных компьютеров от несанкционированное доступа Вы знаете?
1) недопущение нарушителя к вычислительной среде;
2) защита вычислительной среды;
3) использование специальных средств защиты информации ПК от несанкционированного доступа;
4) все вышеперечисленные;
5) правильного ответа нет.

Вопрос 19. Какие средства защиты информации в ПК наиболее распространены?
1) применение различных методов шифрования, не зависящих от контекста информации;
2) средства защиты от копирования коммерческих программных продуктов;
3) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
4) защита от компьютерных вирусов и создание архивов;
5) все вышеперечисленные.

Вопрос № 20. На какие группы делятся информационные ресурсы государства?
1) информация открытая, информация запатентованная и информация, "закрываемая" ее собственником, владельцем и защищаемая им с помощью

отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны
2) информация открытая и информация запатентованная
3) отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

Вопрос № 21. Кто является собственником защищаемой информации?
1) юридическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
2) юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
3) физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

Вопрос № 22. Одной из проблем защиты информации является…
1) классификация возможных каналов утечки информации
2) ее разнообразие
3) ее доступность

Вопрос № 23. К каналам утечки относятся…
1) хищение носителей информации; чтение информации с экрана ПЭВМ посторонним лицом; чтение информации из оставленных без присмотра распечаток программ; подключение к устройствам ПЭВМ специальных аппаратных средств, обеспечивающих доступ к информации;
2) использование технических средств для перехвата электромагнитных излучений технических средств ПЭВМ; несанкционированный доступ программ к информации; расшифровка программой зашифрованной информации; копирование программой информации с носителей.
3) все вышеперечисленное

Вопрос № 24. Известно, что информация - это сведения о…
1) предметах, объектах
2) явлениях и процессах, отображаемые в сознании человека или на каком-либо носителе, для последующего их восприятия человеком
3) все вышеперечисленное

Вопрос № 25. Информационная коммуникация предполагает…
1) обмен между субъектами отношений в виде совокупности процессов представления, передачи и получения информации
2) доступность информации и ее разнообразие
3) все вышеперечисленное

Вопрос № 26. Основные положения современной концепции защиты информации можно свести к следующим положениям:

1) защита информации в государстве должна обеспечить информационную безопасность личности, общества и государства
2) защита должна обеспечить охрану информационных ресурсов страны
3) все вышеперечисленное

Вопрос № 27. Особенности защиты персональных компьютеров (ПК) обусловлены…
1) спецификой их использования
2) частотой процессора
3) все вышеперечисленное

Вопрос № 28. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили…
1) средства, использующие парольную идентификацию и методы шифрования; средства защиты от копирования программных продуктов; защита от компьютерных вирусов и создание архивов.
2) ограничение доступа к персональному компьютеру
3) все вышеперечисленное

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВО 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 деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ОСНОВНАЯ ЛИТЕРАТУРА

1. 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
2. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с.— Режим доступа: http://www.iprbookshop.ru/12014

3. Рудинский И.Д. Технология проектирования автоматизированных систем обработки информации и управления [Электронный ресурс]: учебное пособие/ Рудинский И.Д.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 304 с.— Режим доступа: http://www.iprbookshop.ru/12057
4. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5. Аверченков В.И. Защита персональных данных в организации [Электронный ресурс]: монография/ Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 124 с.— Режим доступа: http://www.iprbookshop.ru/6993
6. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936
7. Зайцев А.П. Технические средства и методы защиты информации [Электронный ресурс]: учебник/ Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 442 с.— Режим доступа: http://www.iprbookshop.ru/12053

ПЕРИОДИЧЕСКИЕ ИЗДАНИЯ

8. Информационная безопасность регионов : науч.-техн. журнал. - Саратов : Изд-во СГСЭУ, 2007 - . - Выходит раз в два месяца. - ISSN 1995-5731
9. Информационные технологии :теорет. и прикл. науч.-техн. журн. - М. : Новые технологии, 1995 - . - Выходит ежемесячно. - ISSN 1684-640

ИНТЕРНЕТ-РЕСУРСЫ

10. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Режим доступа: http://fstec.ru/ Дата обращения 25.08.2015
11. Все об информационных системах персональных данных. Режим доступа: http://ispdn.ru Дата обращения 25.08.2015
12. Росстандарт. Режим доступа: http://www.gost.ru/ Дата обращения 25.08.2015

Источники ИОС

13. Создание автоматизированных систем в защищенном исполнении :https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.03.01/Lists/List/AllItems.aspx

16. Материально-техническое обеспечение

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

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

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

Для проведения лабораторных занятий и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория каф. ИБС, оснащенная компьютерами.

Для проведения лабораторных занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор IntelPentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт. Компьютеры должны иметь подключение к локальной сети СГТУ и доступ к сети Интернет.

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

1. Операционные системы: WindowsXP/7 в составе DreamsParkPremiumMS ИНЭТМ (Windows, VisualStudio), UbuntuLinux.
2. Средства разработки программ: MicrosoftVisualStudioExpress в составе DreamsParkPremiumMS ИНЭТМ, среда разработки NetBeans.
3. Антивирусные средства защиты KasperskyEndpointSecurity для Windows, Антивирус Касперского 6.0 для WindowsWorkstations.
4. Архиватор RARLabsWinRAR.
5. Офисный пакет MicrosoftOffice Профессиональный плюс 2007 для подготовки и оформления отчетов.

Для проведения тестирования используется система тестирования знаний Ast-Test версия 3.