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

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

форма обучения – очная
курс –4
семестр – 8
зачетных единиц – 4
часов в неделю – 6
всего часов – 144
лекции – 18
практические занятия – 36
самостоятельная работа – 90
экзамен – 8 семестр
зачет – 8 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 ВПО

Дисциплина "Оценка информационной безопасности автоматизированных систем в защищенном исполнении" 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:

"*Правовое государство: история и современность*" и «*Организационное и правовое обеспечение информационной безопасности*» – 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;

"*Сети и системы передачи информации*" и *«Управление информационной безопасностью»* – 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:

- способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6),
- способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10),
- способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

Индекс ПК-10	**Формулировка: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности**
Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительно)	**Знает**: - основные актуальные нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - принципы оценки средств информационной безопасности, **Умеет**: - анализировать классифицировать и применять на практике основные нормативно-правовые документы; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками практического применения нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.
Продвинутый (хорошо)	**Знает**: - основные актуальные нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, **Умеет**: - анализировать классифицировать и применять на практике основные нормативно-правовые документы; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками практического применения нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - 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-10	**Формулировка: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности**
Высокий (отлично)	**Знает**: - основные актуальные нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: - анализировать классифицировать и применять на практике основные нормативно-правовые документы; - 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 практического применения нормативно-правовые документы, необходимые для решения задач в профессиональной сфере; - 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-12	**Формулировка: способность принимать участие в проведении экспериментальных исследований системы защиты информации**
Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительно)	**Знает**: - особенности проведения экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - принципы оценки средств информационной безопасности, **Умеет**: - проводить экспериментально-исследовательские работы в системе защиты информации с учетом требований по обеспечению информационной безопасности; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками проведения экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.
Продвинутый (хорошо)	**Знает**: - - особенности проведения экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, **Умеет**: - проводить экспериментально-исследовательские работы в системе защиты информации с учетом требований по обеспечению информационной

Индекс ПК-12	**Формулировка: способность принимать участие в проведении экспериментальных исследований системы защиты информации**
	безопасности; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками проведения экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - 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 проведения экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: - проводить экспериментально-исследовательские работы в системе защиты информации с учетом требований по обеспечению информационной безопасности; - 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 экспериментально-исследовательских работ в системе защиты информации с учетом требований по обеспечению информационной безопасности; - 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-6	**Формулировка: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации**
Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительно)	**Знает**: - принципы организации и сопровождения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - принципы оценки средств информационной безопасности, **Умеет**: - проводить и сопровождать контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты

Индекс ПК-6	**Формулировка:** **способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации**
	информации; - применять имеющиеся знания в области оценки средств информационной безопасности. **Владеет**: - навыками проведения и сопровождения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - необходимым объемом знаний и практических навыков в области оценки средств информационной безопасности.
Продвинутый (хорошо)	**Знает**: - принципы организации и сопровождения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - проводить и сопровождать контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - применять имеющиеся знания в области оценки средств информационной безопасности; - анализировать возможные варианты угроз и примерные портреты нарушителей безопасности системы. **Владеет**: - навыками проведения и сопровождения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - 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**: - принципы организации и сопровождения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - принципы оценки средств информационной безопасности; - возможные варианты угроз и примерные портреты нарушителей безопасности системы, - принципы разработки и внедрения АСЗИ, **Умеет**: - проводить и сопровождать контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - 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 и сопровождения контрольных проверок

Индекс ПК-6	**Формулировка:** **способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации**
	работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - 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.

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

№ мо-ду-ля	№ неде-ли	№ те-мы	Наименование темы	Часы				
				Всего	Лекции	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
8 семестр								
1	1	1	Введение. Подходы и общая характеристика видов оценки информационной безопасности автоматизированных систем в защищенном исполнении. Обзор общих критериев оценки	28	4	-	8	16
2	4	2	Представление общих критериев оценки	26/2	6/2	-	8	12
3	5-6	3	Использование общих критериев	40/4	4/2	-	10/2	26
4	7-9	4	Эффективность проведения оценки и методы ее повышения	50/4	4/2	-	10/2	36
Всего				144/10	18/6	-	36	90

5.Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	4	1	**Подходы и общая характеристика видов оценки информационной безопасности автоматизированных систем в защищенном исполнении.** Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Область применения. Обзор общих критериев оценки. Использование общих критериев потребителями, разработчиками, оценщиками изделий информационных технологий	1-5, 15
2	6/2	2	**Представление общих критериев оценки** Средства построения наборов требований безопасности Функциональные требования безопасности. Требования доверия к безопасности. Зависимости и операции. Пакеты. Профили защиты. Понятие профиля защиты. Содержание профиля защиты. Необходимость профилей защиты. Поиск профилей защиты. Регистрация профилей защиты. Задание по безопасности. Понятие задания по безопасности. Содержание задания по безопасности. Необходимость задания по безопасности. Использование заданий по безопасности. Общая методология оценки. Руководство ИСО по разработке профилей защиты и заданий по безопасности.	1-5, 15
3	4/2	4	**Использование общих критериев** Разработка профилей защиты. Разработка профиля защиты системы, основанной на сертифицированных в соответствии с Общими критериями продуктах информационных технологий. Использование Общих критериев для выбора продуктов и систем информационных технологий.	1-4, 15
4	4/2	4	**Эффективность проведения оценки и методы ее повышения** Интерпретация результатов оценки.	2-4, 15

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
			Сертификация профилей защиты. Каталог сертифицированных продуктов. Результаты оценки. Соотнесение процессов аттестации и сертификации. Выполнение оценки. Стадии выполнения оценки. Виды надзора. Превышение времени оценки над циклом разработки. Стоимость оценки. Взаимное признание оценок	

Интерактивные формы обучения

№ темы	Применяемые технологии интерактивного обучения	Кол-во аудиторных часов
2	Лекция в интерактивном режиме. Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	2
3	Лекция в интерактивном режиме. Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	2
4	Лекция в интерактивном режиме. Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	2

6.Содержание коллоквиумов

Проведение коллоквиумов учебным планом не предусмотрено.

7. Перечень практических работ

Практические занятия выполняются по индивидуальному графику группами, состоящими из 2- 3 студентов. За период обучения студент выполняет **4** работы в соответствии с графиком, разработанным для каждой группы.

№ темы	Всего часов	Наименование работы. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4
1	8	Изучение и анализ профилей защиты, "Контролируемый доступ", "Меточная защита", "Средства защиты ресурсов компьютера от несанкционированного доступа на начальном этапе его загрузки". Изучение и анализ профилей защиты "Операционные системы", "Одноуровневые операционные системы", "Многоуровневые операционные системы", "Операционные системы. Клиентские операционные системы"	1-6, 15

№ темы	Всего часов	Наименование работы. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
2	8	Изучение и анализ профиля защиты "Системы управления базами данных". Изучение и анализ профилей защиты "Межсетевые экраны корпоративного уровня", "Межсетевые экраны провайдерского уровня"	2-7, 15
3	10/2	Изучение и анализ профиля защиты "Удостоверяющие центры инфраструктуры открытых ключей"	1-3, 7-9, 15
4	10/2	Изучение и анализ профилей защиты "Средства построения виртуальных локальных вычислительных сетей", "Средства построения виртуальных частных вычислительных сетей"	5-9, 15

Каждая лабораторная работа представлена в следующем виде:

- цель работы;
- краткие сведения из теории;
- задания;
- контрольные вопросы.

Порядок выполнения лабораторной работы:

1. Изучить информационные материалы к занятию, включая рекомендованную литературу и лекции.
2. Изучить словесную постановку задачи;
3. Выбрать метод, который лучше всего подходит для решения поставленной задачи;
4. Проанализировать различные источники содержащие необходимые сведения для решения поставленной задачи;
5. Оформить результаты поиска в виде реферата;
6. Представить к защите отчет по работе.

Содержание отчета

1. Название лабораторной работы.
2. Цель работы.
3. Словесная постановка задачи.
4. Алгоритм решения задачи.
5. Обоснование правильности выбора алгоритма.
6. Ответы на контрольные вопросы по согласованию с преподавателем.

В рамках проведения лабораторных работ используются интерактивные формы обучения

Для достижения планируемых результатов освоения дисциплины используются следующие образовательные технологии:

Информационно-развивающие технологии:

– лекционно-семинарский метод;

– самостоятельное изучение литературы;

– использование электронных средств информации.

Деятельностные практико-ориентированные технологии:

– анализ конкретных производственных ситуаций;

– контекстное обучение;

Развивающие проблемно-ориентированные технологии:
– проблемные лекции;
– проектная деятельность в группах.

Методы	Лекция	Практическое занятие в т.ч. в интерактивной форме	СРС
Метод IT	+	-	-
Работа в команде	-	+	-
Case-study	+	+	+
Проблемное обучение	+	+	+
Контекстное обучение	+	+	-
Опережающая самостоятельная работа	-	+	+
Индивидуальное обучение	-	+	+

Интерактивные формы обучения

№ работы	Применяемые технологии интерактивного обучения	Кол-во аудиторных часов
3	Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	2
4	Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	2

8. Перечень лабораторных занятий

Лабораторные занятия учебным планом не предусмотрены.

9.Задания для самостоятельной работы студентов

№ темы	**Всего Часов**	**Вопросы для самостоятельного изучения (задания)**	**Учебно-методическое обеспечение**
1	**2**	**3**	**4**
1	16	Оценочные уровни доверия	10-15
2	12	Классы, семейства и компоненты функциональных требований	10-15
3	26	Классы, семейства и компоненты требований доверия, включаемые в оценочные уровни доверия	13-15
4	36	Классы, семейства и компоненты требований доверия, не включаемые в оценочные уровни доверия	12-15

Виды, график контроля СРС (по решению кафедры УМКС/УМКН).

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

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Темы курсовых работ:

1. Проблема информационной безопасности общества
2. Доступность, целостность и конфиденциальность информации
3. Задачи и уровни информационной безопасности общества и методы их решения
4. Нормативно-правовые основы информационной безопасности в РФ
5. Ответственность за нарушения в сфере информационной безопасности (на примере России и другой страны на выбор).
6. Стандарты информационной безопасности
7. Принципы иерархирования в информационной безопасности
8. Стандарты информационной безопасности распределенных систем
9. Стандарты информационной безопасности в РФ
10. Документы по оценке защищенности автоматизированных систем в РФ
11. Административный уровень обеспечения информационной безопасности
12. Классификация «угроз информационной безопасности»
13. Вирусы как угроза информационной безопасности
14. Классификация компьютерных вирусов
15. Характеристика "вирусоподобных" программ
16. Антивирусные программы
17. Обнаружение неизвестного вируса

Требования к подготовке курсовых работ:

- объем работы – 20-25 л., шрифт 14 Times New Roman, межстрочный интервал 1,5, приложения не ограничены по объему, ссылки со сквозной нумерацией на соответствующих страницах.

- содержание:
- титульный лист, оглавление, введение (2-3 стр) с описанием актуальности темы,
- глава №1 с описанием степени разработанность проблематики, основных подходов к базовым определениям, классификациям, особенности представления информации,
- глава №2 содержит практическую часть (например, сравнительную характеристику, примеры использования систем и методов, особенности применения отдельных элементов ПО конкретных ситуациях и др.),
- заключение, в котором содержатся краткие обзоры изложенной информации,

делаются основные выводы и возможные рекомендации автора,

- список использованной литературы с указанием источников.

К работе могут быть оформлены приложения с уточняющими данными (таблицы, графики, например).

- уровень оригинальности (подтвержденный) – не менее 85%.

Обязательно использование при подготовке изданий из списка рекомендованной литературы и других источников (в том числе актуальной периодики).

Подготовленная работа сдается в печатном и электронном виде, вместе с презентацией выступления. Защита работы сопровождается демонстрацией презентации, студенты готовят выступление на 5 мин с изложением основных элементов работы, выводов, и сопровождают ее презентацией. На дискуссию отводится 2-3 минуты после каждого выступления.

12.Курсовой проект

Курсовой проект учебным планом не предусмотрен.

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

Формирование профессиональных компетенций по дисциплине производится на лабораторных и лекционных занятиях (70%); закрепление достигается при проведении промежуточной аттестации (10%), подготовке и защите курсовой работы (10%), сдаче зачета и экзамена (10%).

Формой *первого этапа* итоговой аттестации при освоении дисциплины является **зачет**. К зачету допускаются студенты, прослушавшие теоретический курс дисциплины, сдавшие домашнюю контрольную работу, а также выполнившие и защитившие не менее 2/3 лабораторных работ.

Зачет проводится в традиционной форме собеседования, которое предполагает ответ студента на 2 вопроса. Преподаватель может задать студенту несколько дополнительных вопросов по проблематике курса для более точного определения объема знаний студента.

Критерии оценивания студентов на **зачете**:

Не зачтено - ответ, демонстрирующий отсутствие знаний по теоретическим вопросам и неумение разрешать проблемные ситуации, связанные с изучением основных стандартов, регламентирующих оценку информационной безопасности автоматизированных систем в защищенном исполнении, также указанная оценка может быть присвоена ответу, в котором содержалось значительное количество неточностей и формальных несоответствий.

Зачтено - ответ, демонстрирующий компетентность при описании усвоенного представления об оценке информационной безопасности АСЗИ, достаточного объема знаний и практических навыков в области оценки средств информационной безопасности, а также способности к анализу возможных вариантов угроз и примерных портретов нарушителей безопасности системы.

Формой *второго этапа* итоговой аттестации при освоении дисциплины является **экзамен**. К сдаче экзамена допускаются студенты, прослушавшие теоретический курс дисциплины, сдавшие домашнюю контрольную работу, выполнившие и защитившие не менее 2/3 лабораторных работ, сдавшие зачет с оценкой «зачтено».

Экзамен проводится в традиционной форме собеседования, которое предполагает ответ студента на 2 вопроса. Преподаватель может задать студенту несколько дополнительных вопросов по проблематике курса для более точного определения объема знаний студента.

Критерии оценивания студентов на экзамене:

- «отлично»: демонстрация всестороннего, систематического и глубокого знания учебно- программного материала по оценке информационной безопасности АСЗИ, достаточного объема знаний и практических навыков в области оценки средств информационной безопасности, умение свободно выполнять теоретические и практические задания, усвоение основной и знакомство с дополнительной литературой, рекомендованной программой, демонстрация умений и навыков в рамках формируемых компетенций на высоком уровне освоения.

- «хорошо»; демонстрация полного знания учебно-программного материала по оценке информационной безопасности АСЗИ, достаточного объема знаний и практических навыков в области оценки средств информационной безопасности, успешное выполнение заданий, усвоение основной литературы, рекомендованной в программе, демонстрация умения и навыков в рамках формируемых компетенций на хорошем уровне освоения, способность к самостоятельному пополнению знания в ходе дальнейшей учебной работы и профессиональной деятельности;

- «удовлетворительно»: демонстрация знаний основного учебно-программного материала по оценке информационной безопасности АСЗИ, объема знаний и практических навыков в области оценки средств информационной безопасности в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, освоение с выполнением заданий, предусмотренных программой, знакомство с основной литературой, рекомендованной программой, демонстрация умений и навыков в рамках формируемых компетенций на достаточном уровне освоения.

Вопросы для зачета

1. Средства построения наборов требований безопасности
2. Функциональные требования безопасности.
3. Требования доверия к безопасности.
4. Зависимости и операции.
5. Понятие профиля защиты. Содержание профиля защиты.
6. Поиск профилей защиты. Регистрация профилей защиты
7. Понятие задания по безопасности. Содержание задания по безопасности.
8. Использование заданий по безопасности
9. Общая методология оценки.
10. Руководство ИСО по разработке профилей защиты и заданий по безопасности.
11. Разработка профиля защиты системы, основанной на сертифицированных в соответствии с Общими критериями продуктах информационных технологий.
12. Использование Общих критериев для выбора продуктов и систем информационных технологий
13. Сертификация профилей защиты. Каталог сертифицированных продуктов. Результаты оценки. Соотнесение процессов аттестации и сертификации.
14. Стадии выполнения оценки. Виды надзора.
15. Стоимость оценки. Взаимное признание оценок.

Вопросы для экзамена

1. Предмет дисциплины «Оценка информационной безопасности автоматизированных систем в защищенном исполнении».
2. Теория и методология оценки информационной безопасности, ее основные понятия.
3. Понятие оценки информационной безопасности, ее виды и критерии.
4. Задачи, методы и средства оценки и защиты информации.
5. Понятие конфиденциальности. Критерии выделения информации ограниченного распространения.

6. Основы проведения оценочных и аналитических исследований.
7. Параметры оценки способов обеспечения защиты информации с точки зрения права.
8. Методы и принципы проведения оценки безопасности в системах обеспечения государственной тайны, служебной тайны, коммерческой тайны.
9. Анализ и оценка угроз информационной безопасности объекта (на примере из практики).
10. Оценка способов регламентации допуска и доступа персонала к конфиденциальной информации.
11. Оценка предупредительных и профилактических мер, направленных на предотвращение разглашения персоналом конфиденциальной информации.
12. Оценка эффективности применяемых средств и методов технической защиты объектов и информации.
13. Программы обнаружения и защиты от вируса.
14. Принципы защиты приложений и баз данных исходя из оценки их эффективности.
15. Способы оценки эффективности организации доступа в СУБД «клиент-сервер».
16. Способы защиты локальной рабочей станции

Тестовые задания по дисциплине

Для проведения тестирования используются тестовые материалы, разработанные в среде АСТ-

14. Образовательные технологии

Для успешного освоения дисциплины применяются различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе. 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 деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии. Общее количество занятий, проводимых в интерактивных формах, - не менее 20%.

На лабораторных занятиях используются активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При изучении данного курса используются следующие интерактивные формы проведения занятий:

• мозговой штурм и групповое обсуждение;

• работа в малых группах при проведении лабораторных работ и решения Case-study (анализ конкретных ситуаций);

• метод портфолио;

• метод проектов;

• метод ПОПС-формула;

• метод «Дерево решений» и др.

Чтение лекций осуществляется с использованием компьютерных презентаций. Компьютеризация упражнений и расчетов по всем темам дисциплины осуществляется в учебном компьютерном классе на персональной вычислительной технике.

15. Перечень учебно-методического обеспечения для обучающихся по дисциплине

Обязательные издания

1. 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

2. Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс]: учебное пособие (Гриф УМО)/ Афанасьев А.А., Веденьев Л.Т., Воронцов А А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 550 с. Режим доступа: http://www.iprbookshop.ru/11978

3. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами [Электронный ресурс]: методические указания к самостоятельной работе студентов. Учебно- методическое пособие/ Бурняшов Б.А.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 55 с.
Режим доступа: http://www.iprbookshop.ru/23077

4. Милославская Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс]: учебное пособие/ Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 166 с
Режим доступа: http://www.iprbookshop.ru/12032

5. 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

Дополнительная литература

6. Аверченков В.И. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 100 с.
Режим доступа: http://www.iprbookshop.ru/6992

7. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.
Режим доступа: http://www.iprbookshop.ru/15845.

8. Воройский Ф.С. Информатика. Новый систематизированный толковый словарь-справочник (Введение в современные информационные и телекоммуникационные технологии в терминах и фактах) [Электронный ресурс] / Воройский Ф.С. - Москва: Физматлит, 2011. - . - ISBN 978-5-9221-0426-5
Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922104265.html

9. Ворона В.А. Концептуальные основы создания и применения системы защиты объектов [Электронный ресурс]: учебное пособие/ Ворона В.А., Тихонов В.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 196 с.
Режим доступа: http://www.iprbookshop.ru/11992

10. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс]: монография (Гриф НИИ, УМО)/ Ефимова Л.Л., Кочерга С.А.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2013.— 239 с.
Режим доступа: http://www.iprbookshop.ru/17677

11. Зиновьева Е.С. Международное управление Интернетом: конфликт и сотрудничество [Электронный ресурс] / Е.С. Зиновьева. - Москва: МГИМО, 2011. - . - ISBN 978-5-9228-0701-2.- 170 с.
Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922807012.html

12. Скудис Эд Противостояние хакерам. Пошаговое руководство по компьютерным

атакам и эффективной защите [Электронный ресурс] / Скудис Эд. - Москва: ДМК-пресс. Пер. с англ. - 512 с.: ил. (Серия "Защита и администрирование")., ISBN 5-94074-170-3 Режим доступа: http://www.studentlibrary.ru/book/ISBN5940741703.html

Периодические издания

13. Вестник компьютерных и информационных технологий [Текст]: науч.-техн. и произв. журн. - М: ООО "Машиностроение», (2010-2012), №1-12. - ISSN 1810-7206
14. Информационные технологии: теорет. и прикл. науч.-техн. журн. - М.: Новые технологии, (2005- 2015), №1-11.- ISSN 1684-6400

Источники ИОС

15. Весь лекционный материал размещен в электронной форме в ИОС направления ИФБС интернет- ресурсов СГТУ имени Гагарина Ю.А.

16. Материально-техническое обеспечение дисциплины.

Преподавание дисциплины ведется в стандартных лекционных аудиториях, оснащенных проекционным оборудованием, и компьютерных классах. Компьютеры объединены в локальную сеть с автоматическим выходом в интернет и корпоративную сеть СГТУ, все студенты имеют доступ к ИОС СГТУ и системе АСТ-тест.

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

– персональный компьютер (в конфигурации не хуже: процессор Intel Core 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);

– проектор (разрешение не менее 1280x1024);

– экран для проектора.

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации, не худшей чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт с установленным в компьютерных классах лицензионным ПО:

DreamsPark Premium MS ИНЭТМ (Windows, Visual Studio) Mathcad 14.0 M011 Microsoft Office Профессиональный плюс 2007 Microsoft SQL Server Express Microsoft Visual Studio Express

ГАРАНТ аэро (Клиент) Текущий Пользователь Система тестирования знаний Ast-Test версия 3 Среда разработки NetBeans