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

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Создание автоматизированных систем
в защищенном исполнении»

форма обучения – очная
курс – 5
семестр – 9
зачетных единиц – 3
часов в неделю – 3
всего часов – 108
лекции – 18
практические занятия – 36
самостоятельная работа – 54
зачет – 9 семестр

1. Цели и задачи дисциплины

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

2. Место дисциплины в структуре ООП ВО

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

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

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

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

"*Разработка и эксплуатация защищенных автоматизированных*

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

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

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

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

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

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

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

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

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

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

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

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

№ модуля	№ недели	№ темы	Наименование темы	Часы				
				Всего	Лекции	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
9 семестр								
1	1-4	1	Введение Обзор общих критериев оценки	24/3	4/2	-	4/1	16
2	5-10	2	Представление общих критериев оценки	32/9	8/4	-	12/5	12
3	11-18	3	Использование общих критериев	52/10	6/4	-	20/6	26
Всего				108/22	18/10	-	36/12	54

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	4/2	1	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. Средства построения наборов требований безопасности. Функциональные требования безопасности. Требования доверия к безопасности. Зависимости и операции. Пакеты	1-5, 15

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
2	8/4	2	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	6/4	3	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. Интерпретация результатов оценки. 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.	1-5, 15

Интерактивные формы обучения

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

6. Содержание коллоквиумов

Проведение коллоквиумов учебным планом не предусмотрено.

7. Перечень практических занятий

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

№ темы	Всего часов	Наименование. Вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4
1	4	Изучение и анализ профилей защиты "Контролируемый доступ", "Меточная защита", "Средства защиты ресурсов компьютера от несанкционированного доступа на начальном этапе его загрузки"	2-5, 15
2	12	Изучение и анализ профилей защиты "Операционные системы", "Одноуровневые операционные системы", "Многоуровневые операционные системы", "Операционные системы. Клиентские операционные системы"	4-6,15
3	10	Изучение и анализ профиля защиты "Системы управления базами данных". Изучение и анализ профилей защиты "Межсетевые экраны корпоративного уровня", "Межсетевые экраны провайдерского уровня"	2-6, 15
3	10	Изучение и анализ профиля защиты "Удостоверяющие центры инфраструктуры открытых ключей". Изучение и анализ профилей защиты "Средства построения виртуальных локальных вычислительных сетей", "Средства построения виртуальных частных вычислительных сетей"	1,3-5, 15

Каждое практическое занятие представлено в следующем виде:

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

Порядок выполнения практического занятия:

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. Тема практического занятия.
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 практических занятий 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

№ занятия	Применяемые технологии интерактивного обучения	Кол-во аудиторных часов
1	Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	1
2	Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	5
3	Работа в команде. Case-study. СРС. Опережающая самостоятельная работа	6

8. Перечень лабораторных работ

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	6-15
2	12	Классы, семейства и компоненты функциональных требований	7-15
3	12	Классы, семейства и компоненты требований доверия, включаемые в оценочные уровни доверия	9-15

3	14	Классы, семейства и компоненты требований доверия, не включаемые в оценочные уровни доверия	8-15

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

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
9 семестр			
1-2	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8, (промежуточная аттестация), зачет
3	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	18, зачет

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

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 (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче зачета (15%).

Формой 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 оценкой информационной безопасности АСЗИ и практических навыков в использовании ее средств.

Зачтено - ответ, демонстрирующий компетентность при использовании теоретических и практических элементов оценки информационной безопасности АСЗИ и практических навыков в использовании ее средств, полное знание учебно-программного материала на примере предложенных в билете вопросов, свободно ориентирующийся в основной литературе, продемонстрировавший умения и навыки в

рамках формируемых компетенций на хорошем уровне освоения, способный к самостоятельному пополнению знания в ходе дальнейшей учебной работы и профессиональной деятельности.

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

Экзамен учебным планом не предусмотрен.

Тестовые задания по дисциплине

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

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