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.1.2.7. Безопасность защищенных вычислительных сетей»

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"
Специализация №9 "Создание автоматизированных систем в защищенном исполнении"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 5
часов в неделю – 5
всего часов – 180,
в том числе:
лекции – 32
практические занятия – 48
самостоятельная работа – 100
экзамен – 8 семестр
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: теоретическая и практическая подготовка специалистов в области построения защищенных вычислительных сетей.

Задачи изучения дисциплины:

- изучение основных элементов теории построения защищенных вычислительных сетей;
- изучение основных принципов функционирования средств защиты сетей;
- привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;
- изучение основных угроз в сетях ЭВМ и методов противодействия им;
- овладение механизмами построения защищенных вычислительных сетей.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность защищенных вычислительных сетей» относится к вариативной части блока дисциплин.

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

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Дисциплина «Безопасность защищенных вычислительных сетей» является предшествующей для изучения следующих базовых дисциплин: «Управление

информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности», «Создание автоматизированных систем в защищенном исполнении».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24).

Студент должен знать:

- основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- последовательность и содержание этапов построения компьютерных сетей;
- эталонную модель взаимодействия открытых систем;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ;

Студент должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;
- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;

− эффективно использовать различные методы и средства защиты информации для компьютерных сетей;
− проводить мониторинг угроз безопасности компьютерных сетей;

Студент должен владеть:
− профессиональной терминологией в области информационной безопасности;
− навыками работы с нормативными правовыми актами;
− методами формирования требований по защите информации;
− навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
− навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;
− навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ: межсетевых экранов, систем VPN, систем обнаружения атак, систем-ловушек, сканеров безопасности для защиты сетей.

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

№ модуля	№ недели	№ темы	Наименование темы	Часы/ Из них в интерактивной форме				
				Всего	Лекции	Лабораторные	Практические	СРС
1	2	3	4	5	6	7	8	9
8 семестр								
1	1	1	Вводная часть	4	2	-	2	-
1	2	2	Межсетевое экранирование	28/8	6/6	-	10/2	12
1	4	3	Системы построения VPN	48/8	10/6	-	6/2	32
2	9	4	Системы обнаружения атак	26/8	6/6	-	6/2	14
2	12	5	Системы анализа защищенности	34/10	4/4	-	16/6	14
2	15	6	Системы-ловушки	16/2	2	-	4/2	10
2	17	7	Архитектура защищенной сети	24	2	-	4	18
Всего				180/36	32/24	-	48/12	100

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	Введение: современные методы и средства сетевой защиты	1, 2, 3, 32
2	2	2	Межсетевые экраны, их классификация, основные функции	3, 4, 5, 32
2	2	3	Способы размещения межсетевых экранов в сети	
2	2	4	Системы контроля контента, их функциональные возможности	
3	2	5	Системы построения виртуальных частных сетей (VPN), их классификация, основные функции	5, 8, 9, 32
3	2	6	Варианты построения, реализации, размещения средств VPN	
3	2	7	Протоколы VPN канального уровня: PPTP, L2TP, L2F	
3	2	8	Протоколы VPN сетевого уровня: IPSec (IKE, AH, ESP), SKIP	
3	2	9	Протоколы VPN сеансового уровня: SSL, TLS	
4	2	10	Системы обнаружения атак, их классификация, основные функции	5, 8, 9, 32
4	2	11	Основные режимы работы ПО Snort	
4	2	12	Способы размещения системы обнаружения атак в сети	
5	2	13	Снифферы: разновидности, особенности применения, способы обнаружения	10, 11, 12, 14, 32
5	2	14	Системы анализа защищенности (сканеры безопасности)	
6	2	15	Обманные системы, их классификация, основные функции. Способы размещения обманных систем в сети	10, 11, 12, 14, 32
7	2	16	Разработка типовой архитектуры безопасности локальной вычислительной сети	4, 5, 11, 12, 14, 20, 21, 32

6. Содержание коллоквиумов

Коллоквиумы учебным планом не предусмотрены.

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	Построение схемы архитектуры локальной сети	5, 8, 9, 10, 11, 12, 14
2	4	2	Модели применения межсетевых экранов. Подробная настройка МСЭ	5, 8, 9, 10, 11, 12, 14
2	6	3	Установка и настройка системы мониторинга и	5, 8, 9, 10, 11, 12, 14

			архивирования почтовых сообщений «Дозор-Джет»	
3	6	4	Настройка служб и сервисов Windows Server для построения VPN на базе протокола IPSec	5, 8, 9, 10, 11, 12, 14
4	6	5	Установка и настройка различных режимов работы системы обнаружения атак Snort. Использование сторонних утилит для настройки и наглядного представления результатов	5, 8, 9, 10, 11, 12, 14
5	4	6	Использование сниффера WireShark для обнаружения проблем в работе сети	5, 8, 9, 10, 11, 12, 14
5	6	7	Использование утилит перехвата паролей в локальной сети. Способы обнаружения парольных снифферов в локальной сети	5, 8, 9, 10, 11, 12, 14
5	4	8	Примеры реализации атак на «отказ в обслуживании» и способы противодействия им	5, 8, 9, 10, 11, 12, 14
5	2	9	Использование сканера безопасности Nessus	5, 8, 9, 10, 11, 12, 14
6	4	10	Установка и настройка обманной системы HoneyD и анализ результатов ее работы.	5, 8, 9, 10, 11, 12, 14
7	4	11	Разработка типовой политики безопасности	5, 8, 9, 10, 11, 12, 14

8. Перечень лабораторных работ

Лабораторные работы учебным планом не предусмотрены.

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
2	12	Настройка IP Tables	4, 7, 9, 10, 11, 13, 14, 18, 19, 20, 21, 22, 29, 30, 31, 32
3	14	Настройка протокола IPSec в Windows Server	
3	18	Настройка Web-сервера Apache для работы через протокол SSL	
4	14	Изучение конфигурационных файлов системы обнаружения атак Snort	
5	14	Установка и настройка сканера безопасности XSpider	
6	10	Конфигурация системы HoneyD	
7	18	Анализ типовых архитектур защищенной сети	

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

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
8 семестр			
1-3	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), экзамен
4-7	Работа с печатными источниками, разбор	Рубежный контроль, промежуточный контроль,	Экзамен

	типовых заданий	самоконтроль	

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [32].

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 (модулю)

Изучение дисциплины направлено на формирование следующих компетенций: ПК-10, ПК-24.

Карта компетенции ПК-10: способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	С.1.2.7 «Безопасность защищенных вычислительных сетей»	Знает: -место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в	Лекции Самостоятельная работа Семинары	Тестирование

		области защиты информации; - организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;		
		Умеет: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - профессиональной терминологией в области информационной безопасности; - навыками работы с нормативными правовыми актами; - методами формирования требований по защите информации.	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

Карта компетенции ПК-24: способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	С.1.2.7 «Безопасность защищенных вычислительных сетей»	Знает: - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - основные нормативные правовые акты в области обеспечения информационной	Лекции Самостоятельная работа Практические занятия	Тестирование

		безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; - автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - принципы формирования политики информационной безопасности в автоматизированных системах;		
		Умеет: -разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - планировать политику безопасности информационных систем; - разрабатывать частные политики информационной безопасности автоматизированных систем; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - профессиональной терминологией в области информационной безопасности - навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

		компоненты автоматизированных систем на русском и иностранном языках; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.		

Формирование профессиональных компетенций по дисциплине производится на практических и лекционных занятиях (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче зачета и экзамена (15%).

При выставлении экзаменационных оценок преподаватель руководствуется следующим:

- оценки «отлично» заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на высоком уровне освоения. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины и их значение для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценки «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе, 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;

- оценки «удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, освоившийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «удовлетворительно» выставляется студенту, допустившему неточность в ответе на экзамене;

- оценка «неудовлетворительно» 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 «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессио-

нальной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для зачета

1. Сравнительный анализ современных программных межсетевых экранов.
2. Сравнительный анализ программно-аппаратных межсетевых экранов
3. Сравнительный анализ протоколов туннелирования трафика в канале передачи
4. Сравнительный анализ современных программных систем построения VPN
5. Сравнительный анализ программно-аппаратных систем построения VPN
6. Сравнительный анализ функциональных возможностей современных сканеров безопасности (защищенности)
7. Сравнительный анализ современных систем обнаружения атак
8. Сравнительный анализ современных обманных систем (HoneyPot и др.)
9. Формирование политики безопасности корпоративной сети
10. Сравнительный анализ систем контекстной фильтрации для защиты от утечек конфиденциальной информации
11. Разработка типовой архитектуры безопасности корпоративной сети

Вопросы для экзамена

1. Функциональные возможности сниффера WireShark. Фильтры отображения пакетов. Анализ сетевых протоколов.
2. Перехват трафика с помощью атаки ARP Poison. Защита от атак типа ARP Poison.
3. Коммутаторы: функции Port Security, IP-MAC-Port Binding
4. Коммутаторы: настройка VLAN на основе портов
5. Коммутаторы: настройка VLAN на основе стандарта 802.1Q
6. Коммутаторы: протокол GVRP
7. Коммутаторы: настройка асимметричных VLAN
8. Коммутаторы: настройка статического и динамического агрегирования каналов
9. Коммутаторы: протокол связующего дерева STP
10. Протоколы безопасности в WiFi-сетях.
11. Классификация межсетевых экранов (приказ ФСТЭК №9 от 9 февраля 2016 г.) Соответствие классов сертифицированных МСЭ уровням защищенности персональных данных.
12. МСЭ: Пакетные фильтры, их достоинства и недостатки
13. МСЭ: Шлюзы сеансового уровня, их достоинства и недостатки
14. МСЭ: Контроль прикладного уровня, их достоинства и недостатки
15. МСЭ: Инспекторы состояния (Stateful Inspection), их достоинства и недостатки
16. Дополнительные функциональные возможности межсетевых экранов: трансляция сетевых адресов, отображение портов, аутентификация пользователей, регистрация событий
17. Сертифицированные аппаратные межсетевые экраны
18. Способы подключения межсетевого экрана. Достоинства и недостатки различных вариантов.
19. Системы контроля содержания, их функциональные возможности, достоинства и недостатки. Технологии DPI

20. Классификация систем обнаружения вторжений (приказ ФСТЭК №638 от 6 декабря 2011 г.). Соответствие классов сертифицированных СОВ уровням защищенности персональных данных.
21. Технологии обнаружения вторжений: сигнатурный анализ и обнаружение аномалий
22. Типовая архитектура системы обнаружения вторжений в локальной сети.
23. Сертифицированные системы обнаружения вторжений
24. Основные режимы функционирования СОВ Snort.
25. Синтаксис описания правил анализа пакетов СОВ Snort.
26. Функциональные возможности СОВ OSSEC.
27. Функциональные возможности СОВ Suricata.
28. Классификация обманных систем.
29. Способы размещения обманной системы в локальной сети. Достоинства и недостатки различных вариантов.
30. Анализ защищенности информационных систем. Использование сканера безопасности XSpider.

Тестовые задания по дисциплине

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

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.

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

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Алешин Л.И. Информационные технологии: учеб. пособие / Л.И.Алешин. - М.: Маркет ДС, 2011. - 384 с. Экземпляры всего: 22.
2. Мельников В.П. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf

3. Губенков А.А. Обеспечение безопасности персональных данных: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А.А. Губенков. - Саратов: СГТУ, 2015. - 84 с. Экземпляры всего: 3.
4. Губенков А.А. Обеспечение безопасности персональных данных [Электронный ресурс]: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А.А. Губенков; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2015. - 1 эл. опт. диск (CD-ROM). - ISBN 978-5-7433-2786-7. Электронный аналог печатного издания. Режим доступа: http://lib.sstu.ru/books/zak 51_15.pdf

Дополнительные издания

5. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Саратов: СГТУ, 2010. - 96 с. Экземпляры всего: 40.
6. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей [Электронный ресурс]: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2010. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 260_10.pdf
7. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов : СГТУ, 2009. - 88 с. Экземпляры всего: 2.
8. Губенков, А. А. Информационная безопасность вычислительных сетей [Электронный ресурс]: учеб. пособие / А.А. Губенков; Сарат. гос. техн. ун-т (Саратов). - Электрон. текстовые дан. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 479_09.pdf
9. Терещенко С. Н. Информационная безопасность и защита информации : учеб. пособие / С. Н. Терещенко. - Саратов : СГТУ, 2009. - 136 с. Экземпляры всего: 3.
10.Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М.: Академия, 2006. – 240 с. Экземпляры всего: 19.
11. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - М. : ИЦ "Академия", 2005, 2006, 2007, 2008. - 256 с. Экземпляры всего: 33.
12. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для вузов / П.Н. Девянин. - М.: ИЦ "Академия", 2005. - 144 с. Экземпляры всего: 12.
13. Правовое обеспечение информационной безопасности : учеб. пособие для вузов / С.Я. Казанцев, О.Э. Згаздай, Р.М. Оболенский и др.; под ред. С.Я. Казанцева. - М.: ИЦ "Академия", 2008. - 240 с. Экземпляры всего: 10.
14. Бузов Г.А. Защита от утечки информации по техническим каналам : учеб. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 416 с. Экземпляры всего: 5.

15. Шумский А.А. Системный анализ в защите информации: учеб. пособие / А.А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2005. - 224 с. Экземпляры всего:10.
16. Расторгуев С.П. Основы информационной безопасности: учеб. пособие / С.П. Расторгуев. - М.: ИЦ "Академия", 2007. - 192 с. Экземпляры всего: 8.

Методические указания для обучающихся по освоению дисциплины

17.Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Электронный ресурс]: метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib. sstu.ru/books/zak 88_08.pdf.
18.Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Текст]: метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - 16 с. Экземпляры всего: 5.
19. Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib.sstu.ru/books/zak 87_08.pdf.
20.Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т ; сост.: А.А. Губенков. - Саратов : СГТУ, 2008. - 18 с. Экземпляры всего: 5.
21.Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост. А.А. Губенков. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). - Режим доступа: http://lib. sstu.ru/books/zak 149_09.pdf.
22. Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т (Саратов) ; сост. А.А. Губенков. - Саратов : СГТУ, 2009. - 16 с. Экземпляры всего: 5.

Периодические издания

23.Вестник Саратовского государственного технического университета: науч.-техн. журнал. - Саратов: Изд-во СГТУ, (2003-2015). - ISSN 1999-8341. Режим доступа: http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan
24.Инновационная деятельность: науч.-аналит. журнал. - Саратов: Саратовский ГТУ им. Ю. А. Гагарина, (2010-2015). - ISSN 2071-5226. Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/
25.Журнал «Инновации + Паблисити». Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/

26.Журнал «BIS Journal - Информационная безопасность банков». Режим доступа: https://journal.ib-bank.ru.

Интернет-ресурсы

27. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
28. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. URL:http://www.securitylab.ru/ (дата обращения: 1.06.2015).
29. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
30. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
31. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

32. Весь лекционный материал размещен в электронной форме в ИОС специальности ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А. https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.05.03/C.1.2.8/default.aspx - лекционный материал за 8 семестр.

16. Материально-техническое обеспечение дисциплины.

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 Intel Pentium или AMD 2 ГГц, 2 ОЗУ Гбайта, 320 Гбайт НЖМД);
- проектор (разрешение не менее 1024x768);
- экран для проектора.

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

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium 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 практических занятий в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционные системы: Windows XP/7 в составе DreamsPark Premium MS ИНПИТ (Windows, Visual Studio), Ubuntu Linux.

2. Средства разработки программ: Microsoft Visual Studio Express в составе DreamsPark Premium MS ИНЭТМ, среда разработки NetBeans.

3. Антивирусные средства защиты Kaspersky Endpoint Security для Windows, Антивирус Касперского 6.0 для Windows Workstations.

4. Свободно распространяемые средства построения виртуальных машин. Например: VMWare Player или Virtual Box.

5. Архиватор RARLabs WinRAR.

6. Офисный пакет Microsoft Office Профессиональный 2010 для подготовки и оформления отчетов.

7. Свободно распространяемые программные анализаторы протоколов. Например: WireShark, Ethereal.

8. Свободно распространяемое средство обнаружения вторжений Snort, Suricata, OSSEC.

9. Свободно распространяемый пакет IPTABLES в составе Linux или другой МСЭ.

10. Свободно распространяемые системы-ловушки HoneyPot, сканеры безопасности Microsoft Safety Scanner, Nessus, XSpider.

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