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.1.1.20 Безопасность сетей ЭВМ»

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

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 5
часов в неделю – 4
всего часов – 180,
в том числе:
лекции – 32
практические занятия – 32
самостоятельная работа – 116
экзамен – 7 семестр
курсовая работа – 7 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей, а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Дисциплина является базовой для изучения дисциплин по комплексному и организационному обеспечению информационной безопасности.

Задачи изучения дисциплины:

- изучение архитектуры вычислительных сетей;
- изучение программно-аппаратных и технических средств создания сетей;
- изучение принципов построения сетей и управления ими;
- изучение правил организационной, технической и правовой защиты;
- изучение основ использования программных и аппаратных технологий защиты сетей;
- изучение методологии проектирования, развертывания и сопровождения безопасных сетей;
- знакомство с методологией обследования и анализа защищенных вычислительных сетей.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность сетей ЭВМ» относится к к базовой 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 сетей ЭВМ» является предшествующей для изучения следующих базовых дисциплин: «Управление информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности», «Безопасность защищенных вычислительных сетей».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

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

Студент должен знать:

- 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 области защиты информации;
- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- основные протоколы компьютерных сетей;
- последовательность и содержание этапов построения компьютерных сетей;
- эталонную модель взаимодействия открытых систем;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
- методологические и технологические основы обеспечения информационной безопасности сетевых автоматизированных систем;
- угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;

- типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения;
- роль человеческого фактора в обеспечении безопасности сетей;
- возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях;
- принципы функционирования основных защищенных сетевых протоколов;
- основы применения межсетевых экранов для защиты сетей;
- правила определения политики сетевой безопасности;

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;
- 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;
- проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации в автоматизированных системах;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты информации в сетях;
- реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
- реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

Студент должен владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативными правовыми актами;
- навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;

− навыками использования программно-аппаратных средств обеспечения сетей;
− навыками построения и эксплуатации вычислительных сетей;
− навыками комплексного анализа и оценки сетевой безопасности.

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

№ Мо-ду-ля	№ Не де ли	№ Те мы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лек-ции	Коллок-виумы	Лабора-торные	Прак-тичес-кие	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
7 семестр									
1	1	1	Этап предварительного сбора данных.	24	4	-	-	-	20
1	4	2	Методы сканирования сетей.	52/8	16/4	-	-	12/4	24
2	8	3	Определение версии операционной системы и сетевых служб.	40/6	6/6	-	-	8	26
2	10	4	Получение информации через службу NETBIOS в ОС Windows	36/8	4/6	-	-	8/2	24
2	15	5	Способы удаленного подбора паролей	28/6	2/2	-	-	4/4	22
Всего				180/28	32/18	-	-	32/10	116

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	Этап предварительного сбора данных. Использование сервиса WhoIs.	1, 2, 9, 10, 17, 18, 19, 32
1	2	2	Использование программы nslookup для работы с DNS серверами. Перенос зоны DNS-сервера. Получение расширенной информации. Получение списка почтовых серверов.	
2	4	3	Методы сканирования сетей. Сканирование сети с помощью утилиты ping.	1, 2, 4, 5, 6, 7, 32

			Автоматизированный ping. Использование fping. Использование утилиты Nmap. Использование утилиты Pinger. Блокировка ping-сканирования.	
2	2	4	Другие типы пакетов ICMP. Сканирование с помощью различных типов ICMP пакетов. Блокировка ICMP-пакетов. Обнаружение ping-сканирования.	
2	2	5	Сканирование через протокол TCP. Использование программ Nmap и hping2.	
2	2	6	Методы сканирования портов. Методы сканирования TCP connect и SYN Scan.	
2	2	7	Скрытые методы сканирования. Использование графической оболочки ZenMap для Nmap.	
2	2	8	Использование NetScanTools Pro 2000 и SuperScan. Профессиональные сканеры. Использование strobe, FScan, x-port, ipEye.	
2	2	9	Сканирование UDP-портов. Использование udp_scan. Использование WUPS Анализ результатов сканирования.	
3	2	10	Определение типа и версии операционной системы удаленного хоста. Активное определение версии операционной системы. Использование утилит Nmap, queso, Xprobe2, x-port, OSFP. Защита от определения операционной системы. Обнаружение факта сканирования. Предотвращение сканирования.	1, 2, 9, 10, 12, 13, 14, 21, 32
3	2	11	Пассивное определение операционной системы. Использование siphon. Использование p0f.	
3	2	12	Определение производителя и версий сетевых служб. Ручной сбор идентификационных маркеров. Использование Telnet и NetCat. Автоматизированные сборщики идентификационных маркеров. Использование Amap, ScanLine, FScan, Grabbb. Меры по предотвращению сбора идентификационных маркеров.	
4	2	13	Установка нулевого соединения со службой сеансов NETBIOS Протокол SMB и нулевое соединение. Команда net use и работа с общими ресурсами. Инвентаризация пользователей. Использование user2sid + sid2user. Использование SID&User, UserInfo и UserDump, DumpSec. Универсальные средства инвентаризации: enum, nete, Winfo, Winfingerprint, nbtdump. Защита от сбора данных через нулевой сеанс в Windows 2000. Защита от сбора данных через нулевой сеанс в Windows XP.	1, 2, 9, 10, 11, 12, 16, 32

4	2	14	Инвентаризация общих ресурсов. Получение списка общих ресурсов через нулевое соединение. Использование net view и утилит из Resource Kit Использование DumpSec. Автоматические сканеры NetBIOS: Legion и NAT. Инвентаризация системного реестра regdmp и DumpSec. Проверка защищенности системного реестра.	
5	2	15	Способы удаленного подбора паролей. Подбор паролей с локального хоста. Подбор паролей с удаленного сервера. Сборка программы hydra. Опции программы hydra. Подбор пароля к почтовому ящику. Подбор пароля к общим ресурсам.	

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
2	2	1	Построение схемы архитектуры локальной сети	1, 2, 9, 32
2	2	2	Разработка типовой политики безопасности.	1, 2, 9, 32
2	4	3	Модели применения межсетевых экранов	1, 2, 9, 10, 11, 12
2	4	4	Примеры реализации атак на «отказ в обслуживании» и способы противодействия им	1, 2, 9, 10, 11, 12
3	4	5	Анализ и сравнение защитных свойств известных сетевых ОС.	1, 2, 9, 10, 11, 12
3	4	6	Изучение возможностей сканера портов по определению типа ОС.	1, 2, 9, 10, 11, 12
4	8	7	Конфигурирование TCP/IP и настройка коммуникационных каналов. Настройка основных сервисов Internet	10, 11, 12, 32
5	4	8	Безопасность рабочей станции, подключенной к Internet. Управление объектами-группами и пользователями. Установка прав доступа. Дополнительные настройки	10, 11, 12, 32

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
1	20	Протоколы маршрутизации	1, 2, 8, 11, 12, 13, 14, 18, 19, 20, 21, 22, 29, 30, 31, 32
2	24	Протоколы виртуальных частных сетей	
3	26	Общие критерии оценки безопасности информационных технологий	
4	24	Особенности протокола IPv6	
5	22	Нормативно-правовая база электронного документооборота	

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

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
7 семестр			
1-3	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), экзамен
4,5	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Экзамен

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

В рамках учебного плана студенты выполняют курсовую работу по теме: «Анализ уязвимостей в программном обеспечении».

Варианты заданий на курсовую работу содержатся в методических указаниях, размещенных в ИОС СГТУ:

https://portal.sstu.ru/Fakult/FETIP/IBS/%D1%81316_1/default.aspx

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-17, ПК-24.

Карта компетенции ПК-17: способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

№ 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.1.1.20 «Безопасность сетей ЭВМ»	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 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;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;	Практические занятия с использованием активных и интерактивных приемов обучения. Курсовая работа. Самостоятельная работа	Тестирование рефераты

		- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;		
		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. Курсовая работа. 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.1.1.20 «Безопасность сетей ЭВМ»	Знает: - принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; - основные протоколы компьютерных сетей; - последовательность и содержание этапов построения компьютерных сетей; - эталонную модель взаимодействия открытых систем; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - 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	Практические занятия с использованием активных и интерактивных приемов обучения. Курсовая работа. Самостоятельная работа	Тестирование рефераты

		сетей;		
		Владеет: - профессиональной терминологией в области информационной безопасности; - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) 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 сетей;	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Курсовая работа. Самостоятельная работа	Экзамен

Формирование профессиональных компетенций по дисциплине производится на практических и лекционных занятиях (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче 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 профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для зачета

Зачет учебным планом не предусмотрен.

Вопросы для экзамена

1. Основные этапы проведения удаленной атаки на вычислительную сеть. Типы сетевых атак.
2. Этап предварительного сбора данных. Использование открытых источников, типы запросов к службе whois, опции поиска в google.
3. Клиент-серверная система DNS. Типы DNS-серверов. Способы получения сведений с DNS-серверов. Перенос зоны. Атака Каминского.
4. Определение топологии сети. Особенности работы утилит tracert и traceroute.
5. Выявление компьютеров, подключенных к Internet. Типы пакетов ICMP. Способы защиты от сканирования сети.
6. Сканирование портов. Типы сканирования. Защита от сканирования портов.
7. Определение типа и версии операционной системы. Способы активного и пассивного исследования стека TCP/IP. Обнаружение попыток определения операционной системы и их предотвращение.
8. Сбор идентификационных маркеров автоматически и вручную с помощью утилит telnet и netcat. Возможные контрмеры.
9. Инвентаризация службы имен NetBIOS (137 порт). Возможные контрмеры. Протокол LLMNR.
10. Инвентаризация службы сеансов NetBIOS (139 порт). Сбор данных через «нулевое соединение». Возможные контрмеры, запрет установления «нулевого соединения».
11. Протокол SMB, его версии. Уязвимости в протоколе SMB. Возможные меры защиты.
12. Протоколы FTP, SFTP, FTPS. Возможные атаки.
13. Инвентаризация службы SNMP (161 порт). Возможные контрмеры.
14. Способы локального подбора паролей. Возможные контрмеры.
15. Способы удаленного подбора паролей. Возможные контрмеры.
16. Разновидности DDOS-атак сетевого уровня
17. Разновидности DDOS-атак прикладного уровня
18. DDOS-атаки с усилением через промежуточные сервера. Способы защиты.
19. Сканеры безопасности, сравнение их возможностей.

20. Комплекс Metasploit Framework: состав, варианты использования, возможности meterpreter.

Тестовые задания по дисциплине

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

Примеры тестовых заданий:

1. Какое из определений является верным?
   a) Туннелирование в компьютерных сетях – процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.
   b) Туннелирование в компьютерных сетях – постоянное соединение, предоставляемое телекоммуникационной компанией для доступа к Интернету;
   c) Туннелирование в компьютерных сетях – результат одновременной попытки нескольких компьютеров получить доступ к физической среде сети;
   d) Туннелирование в компьютерных сетях – метод передачи данных с возможностью одновременной передачи информации в обоих направлениях (отправка и получение);

2. Что такое VPN?
   a) Голосовой продукт сети;
   b) Доброволец физической сети;
   c) Голосовой продукт безопасности;
   d) Виртуальные частные сети.

3. Какова цель создания VPN?
   a) Обеспечение связи между компьютерами локальной сети без использования Internet;
   b) Обеспечение связи между компьютерами локальной сети с использованием Internet;
   c) Обособление потока данных определенной группы пользователей от потока данных других пользователей общей сети.
   d) Инкапсулирование трафика локальной сети;

4. Выберите протоколы защиты на канальном уровне. (Возможно несколько вариантов)
   a) SSL.
   b) PPTP.
   c) L2F.
   d) L2TP.

5. Выберите протоколы защиты на канальном уровне. (Возможно несколько вариантов)

e) SHTTP.
f) IPSec.
g) SKIP.
h) L2TP.

6. Выберите протоколы защиты на прикладном уровне. (Возможно несколько вариантов)
   a) S/MIME.
   b) PPTP.
   c) SHTTP.
   d) L2TP.

7. Выберите протоколы защиты на транспортном уровне. (Возможно несколько вариантов)
   a) SSL.
   b) TLS.
   c) SOCKS.
   d) L2TP.

8. Какие утверждения верные?
   a) VPN канального уровня обеспечивает инкапсуляцию трафика сетевого и более высоких уровней и построение виртуальных туннелей "точка - точка".
   b) VPN канального уровня осуществляет инкапсуляцию IP в IP;
   c) VPN сетевого уровня осуществляет инкапсуляцию IP в IP.
   d) VPN сетевого уровня обеспечивает инкапсуляцию трафика сетевого и более высоких уровней и построение виртуальных туннелей "точка - точка".

9. Выберите основные компоненты туннеля. (Возможно несколько вариантов)
   a) инициатор туннеля
   b) маршрутизируемая сеть
   c) туннельный коммутатор
   d) туннельный терминатор (или несколько)
10. Какие типы протоколов принимают участие в процессе туннелирования? (Возможно несколько вариантов)
    a) транспортируемый протокол.
    b) несущий протокол.
    c) сетевой протокол.
    d) протокол инкапсуляции.

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 28 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.1.1.20/default.aspx - лекционный материал за 7 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 плюс 2007 для подготовки и оформления отчетов.
7. Свободно распространяемые программные анализаторы протоколов. Например: WireShark, Ethereal.
8. Свободно распространяемое средство обнаружения вторжений Snort или другое средство обнаружения вторжений.
9. Свободно распространяемый пакет IPTABLES в составе Linux или другой межсетевой экран.
10. Свободно распространяемые системы-ловушки HoneyPot, сканеры безопасности Microsoft Safety Scanner.

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