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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

«Б.1.3.12.1 Информационная безопасность Интернет-приложений»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 4
часов в неделю – 7
всего часов – 144,
в том числе:
лекции – 36
коллоквиумы – 8
практические занятия – 33
самостоятельная работа – 67
экзамен – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов основам обеспечения информационной защищённости Интернет-приложений, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных веб-сайтов, а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

- изучение архитектуры Интернет-приложений;
- изучение программно-аппаратных и технических средств создания Интернет-приложения;
- изучение основных методов и программных инструментов, используемых для обеспечения информационной защищённости Интернет-приложений;
- изучение правил организационной, технической и правовой защиты Интернет-приложений;
- знакомство с методологией обследования и анализа защищенных Интернет-приложений;
- получение базовых знаний и практических навыков по поиску и анализу уязвимостей веб-приложений.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность Интернет-приложений» относится к числу дисциплин по выбору.

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.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

Студент должен знать:

- методологические и технологические основы обеспечения информационной безопасности Интернет-приложений;
- угрозы и методы нарушения информационной безопасности Интернет-приложений;
- типовые модели атак, направленных на преодоление защиты Интернет-приложений, условия их осуществимости, возможные последствия, способы предотвращения;
- роль человеческого фактора в обеспечении безопасности Интернет-приложений;
- возможности, способы и правила применения основных программных и аппаратных средств защиты Интернет-приложений;
- принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS);
- основы применения межсетевых экранов для защиты Интернет-приложений;
- правила, процедуры, практические приемы для управления информационной безопасностью;
- методы создания защищённых Интернет-приложений.

Студент должен уметь:

- проводить анализ Интернет-приложений с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты Интернет-приложений;

- реализовывать меры противодействия выявленным угрозам безопасности Интернет-приложений с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
- составлять комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
- реализовывать системы защиты Интернет-приложений в соответствии со стандартами по оценке защищенных систем.

Студент должен владеть:

- навыками работы с нормативно-правовыми актами и методическими документами;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, веб-серверов с учетом требований по обеспечению информационной безопасности;
- навыками проектирования защищенных Интернет-приложений;
- навыками комплексного анализа защищенности Интернет-приложений;
- методами организации и управления деятельностью служб защиты информации на предприятии.

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

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
8 семестр									
1	1	1	Архитектура Интернет-приложений	28/4	4	4/4	-	4	16
1	3	2	Методы аутентификации на веб-сайтах	28/2	6	2	-	10/2	10
2	6	3	Удаленное выполнение команд на веб-сервере	29/4	6	2/2	-	5/2	16
2	9	4	Атаки на клиентов веб-приложения Cross-Site-Scripting	23	4	-	-	8	11
2	11	5	Атаки на базы данных SQL injection	36/2	16	-	-	6/2	14
Всего				**144/12**	**36**	**8/6**	**-**	**33/6**	**67**

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	Тема 1. Архитектура Интернет-приложений. адресация в Интернет, домены, HTML-страницы. Особенности работы CGI-скриптов.	1, 2, 16, 17, 32
1	2	2	Установка, настройка и администрирование веб-сервера. Понятие сокета, конструкция запросов, файловая структура и ведение логов. Frontend- и backend-серверы, использование веб-серверов для получения статического контента и проксирования запросов. Обзор языков, используемых для разработки серверных приложений. Устройство CGI-скриптов и библиотеки для работы с ними.	1, 2, 3, 5, 32
2	2	3	Тема 2. Методы аутентификации на веб-сайтах. Базовая авторизация в протоколе HTTP. Система авторизации с помощью web-форм. Протокол Kerberos.	3, 5, 15, 18, 32
2	2	4	Brute-force атаки на веб-приложения. Технология Captcha.	3, 5, 6, 12, 13, 32
2	2	5	Способы идентификации веб-сервера и браузера клиента. Понятие сессии, файлы cookies.	3, 7, 8, 32
3	2	6	Тема 3. Удаленное выполнение команд на веб-сервере (Remote Code Execution). Структура URL. Кодировка URL. Уязвимость двойного декодирования Unicode.	5, 6, 20, 32
3	2	7	Уязвимость типа Local File Inclusion. Примеры реализации на языке PHP. Права доступа в Linux. Уязвимость типа Remote File Inclusion. Способы защиты.	5, 6, 32
3	2	8	Загрузка произвольных файлов (Unrestricted File Upload). Внедрение веб-шелла и его скрытие на сервере. Загрузка и компиляция эксплойтов. Очистка логов веб-сервера.	5, 6, 21, 32
4	2	9	Тема 4. Атаки на клиентов веб-приложения Cross-Site-Scripting. Синтаксис языка JavaScript, способы подключения к web-странице, модели обработки событий. Технология AJAX. Понятие Same origin policy. Классификация XSS-атак.	5, 6, 7, 8, 32
4	2	10	Межсайтовое выполнение сценариев в Java/Flash-приложениях. Средства безопасности в браузерах. Защита от XSS-атак.	5, 6, 7, 8, 32
5	4	11	Тема 5. Атаки на базы данных SQL injection. Основные понятия реляционных БД, типы данных в SQL и работа с ними (нормализация, управление данными, выборки). Способы проверки целостности базы, использование внешних ключей. Служебные символы языка SQL в распространённых СУБД.	5, 6, 7, 8, 32

5	4	12	Классическая техника эксплуатации уязвимости SQL injection с помощью оператора «UNION»	6, 7, 8, 32
5	4	13	Слепое внедрение операторов SQL (Blind SQL Injection) с помощью оператора «AND»	6, 7, 8, 32
5	4	14	Работа с файловой системой при эксплуатации уязвимости SQL Injection. Выполнение команд на сервере при эксплуатации уязвимости SQL Injection. Time-based атаки.	6, 7, 9, 32

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	Структура запросов и ответов в протоколе HTTP, назначение HTTP-заголовков, коды ответа сервера. Структура заголовка и тела e-mail письма, протоколы SMTP, POP3 и IMAP.	1, 2, 3, 10, 11, 32
1	2	2	Обфускация и защита веб-сайтов. Валидация и очистка входных данных.	3, 5, 19, 32
2	2	3	Протоколы SSL и TLS. Структура сертификата открытого ключа. Инфраструктура открытых ключей PKI	2, 7, 8, 14, 32
3	2	4	Средства автоматического обнаружения уязвимостей Интернет-приложений.	5, 6, 7, 8, 22, 32

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	4	1	Аудит безопасности Web-приложений	3, 5, 6, 32
2	10	2	Обнаружение уязвимостей Web-приложений	3, 5, 6, 7, 8, 32
3	5	3	Удаленное выполнение команд на веб-сервере	3, 5, 6, 7, 8, 32
4	8	4	Обнаружение уязвимостей и реализация XSS-атак на тестовых веб-сайтах	3, 5, 6, 7, 8, 32
5	6	5	Изучение разновидностей атак типа SQL injection на тестовых веб-сайтах.	3, 5, 6, 7, 8, 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	16	Использование обратимого шифрования в Интернет-приложениях.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 32
2	10	Протоколы аутентификации OAuth и OpenID.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 31, 32
3	16	Уязвимость HTTP Parameter Pollution.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 31, 32
4	11	Способы обхода фильтров безопасности и Web Application Firewall.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 31, 32
5	14	Фрагментированные SQL инъекции.	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 29, 30, 31, 32

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

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
4,5	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Экзамен

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

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-7.

Карта компетенции ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
2	Б.1.3.12.1 Информационная безопасность Интернет-приложений	Знает: - методологические и технологические основы обеспечения информационной безопасности Интернет-приложений; - угрозы и методы нарушения информационной безопасности Интернет-приложений; - типовые модели атак, направленных на преодоление защиты Интернет-приложений, условия их осуществимости, возможные последствия, способы предотвращения; - роль человеческого фактора в обеспечении безопасности Интернет-приложений; - возможности, способы и правила применения основных программных и аппаратных средств защиты Интернет-приложений; - принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS); - основы применения межсетевых экранов для защиты Интернет-приложений; - правила, процедуры, практические приемы для управления информационной безопасностью;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты Интернет-приложений; - реализовывать меры противодействия выявленным угрозам безопасности Интернет-приложений с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения; - составлять комплекс мер	Практические работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты

		(правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; - проводить анализ Интернет-приложений с точки зрения обеспечения информационной безопасности; - разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;		
		Владеет: - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, веб-серверов с учетом требований по обеспечению информационной безопасности; - навыками проектирования защищенных Интернет-приложений; - навыками комплексного анализа защищенности Интернет-приложений; - методами организации и управления деятельностью служб защиты информации на предприятии.	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. 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 компетен-

ций 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. Многоуровневая архитектура Web-приложения. Языки программирования и фреймворки для разработки приложений.
2. Протокол HTTP. Структура запроса клиента и ответа сервера. Коды ответов сервера. Средства анализа протокола HTTP.
3. Структура URL. Кодирование URL. Уязвимости избыточного декодирования Unicode. Удаленное выполнение команд.
4. Структура формы в HTML. Элементы ввода данных. Способы передачи параметров. Скрытые поля.
5. Алгоритм базовой аутентификации в протоколе HTTP.
6. Аутентификация, основанная на формах и cookies.
7. Аутентификация и авторизация пользователей сайта через OAuth.
8. Bruteforce-атаки на веб-приложения. Технология Captcha.
9. Уязвимость Local File Include.
10. Уязвимость Remote File Include.
11. Способы загрузки веб-шелла на сервер. Функции веб-шелла.
12. Обфускация PHP-кода и средства его расшифровки.
13. Способы организации полноценного шелла (netcat, back connect shell).
14. Способы локального повышения прав пользователя на веб-сервере.
15. Сокрытие следов присутствия, очистка логов на сервере.
16. Способы защиты от PHP инклудов.
17. Аудит системных событий в Linux
18. Межсайтовый скриптинг XSS. Классификация атак. Понятие Same Origin Policy.
19. Отраженные и хранимые XSS-атаки.

20. DOM Based XSS-атаки.
21. Атака Cross-Site Request Forgery.
22. Способы защиты от XSS-атак.
23. Алгоритм атаки типа SQL injection.
24. Классическая атака SQL-injection с использованием оператора UNION.
25. Слепая атака SQL-injection с использованием оператора AND.
26. SQL-инъекции, использующие временные задержки.
27. Атака расщепления SQL-запроса.
28. Способы защиты от атак типа SQL-injection.
29. Способы организации DDoS-атаки на веб-приложения.
30. Настройка параметров безопасности веб-сервера Apache. Модуль mod_security.

Тестовые задания по дисциплине

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

Примеры тестовых заданий:

1. Выберите неверный ответ. Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:
a) Читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере.
b) Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
c)Использовать захваченный компьютер в целях продажи его на рынке товаров.
d)Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

2. Средства защиты от несанкционированного доступа можно разделить на категорию:
a) Средства ограничения физического доступа.
b) Средства нападения на держателя информации
c) Средства отключения электроэнергии
d) Средства установки антивирусных приложений

3. Выберите неверный ответ. В штатном режиме работы электронный замок получает управление от BIOS защищаемого компьютера после включения последнего. На этом этапе и выполняются все действия по контролю доступа на компьютер, а именно:
a) Замок запрашивает у пользователя носитель с ключевой информацией, необходимой для его аутентификации.
b) Если аутентификация пользователя прошла успешно, замок рассчитывает контрольные суммы файлов, содержащихся в списке контролируемых, и сравнивает полученные контрольные суммы с эталонными.
c) Если все проверки пройдены успешно, замок возвращает управление компьютеру для загрузки штатной операционной системы.
d) Сокрытие всех важных информационных источник, а так же информацию, относящую к государственной тайне.

4. Выберите неверный ответ. Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:
a) Пакет отправляется адресату (по внутренней сети) согласно информации, находящейся в его оригинальном заголовке.
b) С помощью выбранного алгоритма защиты целостности формируется и добавляется в IP-пакет электронная цифровая подпись (ЭЦП), имитоприставка или аналогичная контрольная сумма.
c) С помощью выбранного алгоритма шифрования производится зашифрование IP-пакета.
d) Пакет отправляется VPN-агенту адресата. При необходимости, производится его разбиение и поочередная отправка результирующих пакетов.

5. Выберите неверный ответ. При приеме IP-пакета VPN-агент производит следующее:
a) Выделяется информационная (инкапсулированная) часть пакета и производится ее расшифрование.
b) Производится контроль целостности пакета на основе выбранного алгоритма. В случае обнаружения нарушения целостности пакет отбрасывается.
c) С помощью выбранного алгоритма шифрования производится зашифрование IP-пакета.
d)Пакет отправляется адресату (по внутренней сети) согласно информации, находящейся в его оригинальном заголовке.

6. Политика безопасности является набором правил, согласно которым устанавливаются защищенные каналы связи между абонентами VPN. Такие каналы обычно называют туннелями, аналогия с которыми просматривается в следующем:
a) Вся передаваемая в рамках одного туннеля информация защищена как от несанкционированного просмотра, так и от модификации.
b) Производится контроль целостности пакета на основе выбранного алгоритма. В случае обнаружения нарушения целостности пакет отбрасывается.
c) Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
d) Выделяется информационная (инкапсулированная) часть пакета и производится ее расшифрование.

7. Выберите неверный ответ. Правила создания туннелей формируются в зависимости от различных характеристик IP-пакетов, например, основной при построении большинства VPN протокол IPSec (Security Architecture for IP) устанавливает следующий набор входных данных, по которым выбираются параметры туннелирования и принимается решение при фильтрации конкретного IP-пакета:
a) IP-адрес источника. Это может быть не только одиночный IP-адрес, но и адрес подсети или диапазон адресов.
b) IP-адрес назначения. Также может быть диапазон адресов, указываемый явно, с помощью маски подсети или шаблона.
c) Идентификатор пользователя (отправителя или получателя).
d) Номера протокола, с которого или на который отправлен пакет.

8. Какими функциями обладает межсетевой экран:

a) антивирусное сканирование.
b) подключения к удаленному доступу.
c) сканирование удаленного доступа через ICMP пакеты.
d) идентификация пользователя.

9. Что не относится к комплексной защиты
a) Защита компьютера от физического доступа.
b) Защита компьютера от НСД по сети и организация VPN.
c) Шифрование файлов по требованию.
d) идентификация пользователя.

10. Что не относится к методам и средствам защиты от несанкционированного доступа:
a) Проблема несанкционированного доступа.
b) Проблемы порчи имущества путем физического воздействия.
c) Средства ограничения физического доступа.
d) Средства защиты от НСД по сети.

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 12 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. – 240с. 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 направления ИФБС интернет-ресурсов СГТУ имени Гагарина Ю.А. https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.03.01/B.1.3.11.1/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. Средство анализа защищенности «Сканер безопасности XSpider 7.8».

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

6. Архиватор RARLabs WinRAR.

7. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.

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