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.1.3.12.2 Безопасность электронного бизнеса»

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 является изучение студентами основных видов современных платежных систем, применяемых в России и за рубежом, международных платежных систем, а также современных методов обеспечения безопасности платежных систем.

Задачи изучения дисциплины:

- изучение правовой базы и структуры платежной системы России, электронной системы расчетов Банка России, технологии электронных платежей в расчетной сети Банка России и основ обеспечения ее безопасности,;
- изучение технологий внутрибанковских, межфилиальных, межбанковских и международных расчетов и основ обеспечения их безопасности;
- изучение технологий, применяемых в платежных системах с банковскими картами, и основ обеспечения их безопасности.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность электронного бизнеса» 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:

- виды и способы дистанционного оказания банковских услуг;
- классификацию пластиковых карточек, базовые технологии их использования;
- требования, методы и средства информационной безопасности в технологиях платежных систем;
- правила, процедуры, практические приемы для управления информационной безопасностью.

Студент должен уметь:

- проводить анализ систем электронного бизнеса 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 защиты платежных систем;
- реализовывать меры противодействия выявленным угрозам безопасности платежных систем 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.

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 систем электронного бизнеса;
- навыками комплексного анализа защищенности систем электронного бизнеса;
- 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	Методологические основы информационно-аналитической деятельности	28/4	4	4/4	-	4	16
1	5	2	Платежная система Банка России и ее безопасность	40/2	14	2	-	14/2	10
2	9	3	Прямые межбанковские расчеты и их безопасность	29/4	6	2/2	-	5/2	16
2	13	4	Клиринговые расчеты и их безопасность	19	4	-	-	4	11
2	15	5	Платежные системы с использованием банковских карт и их безопасность	28/2	8	-	-	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. Методологические основы информационно-аналитической деятельности. Предмет, задачи и содержание дисциплины, место дисциплины в системе подготовки инженеров по специальности. Место дисциплины среди смежных дисциплин. Методологические вопросы построения дисциплины. Рекомендации студентам по изучению дисциплины. Правовая база регулирования платежной системы. Особенности реформирования платежной системы. Эволюция расчетной системы России.	1, 2, 3, 11, 19, 21, 32
1	2	2	Банковские технологии совершения безналичных расчетов и их безопасность. Использование новых банковских и финансовых технологий для совершенствования безналичных расчетов.	1, 2, 3, 5, 32

2	4	3	Тема 2. Платежная система Банка России и ее безопасность. Структура платежной системы России. Основные принципы обеспечения безопасности платежной системы России.	3, 5, 6, 7, 8, 10, 11, 32
2	8	4	Основные принципы создания и функционирования электронной системы расчетов Банка России и обеспечения ее безопасности. Порядок осуществления расчетных операций через Банк России и обеспечения их безопасности. Участники платежной системы Банка России. Положение Банка России №672-П от 09.01.2019 «О требованиях к защите информации в платежной системе Банка России» Система быстрых платежей. Меры по противодействию осуществлению переводов денежных средств без согласия клиента в СБП. Меры защиты информации в СПФС. Порядок обеспечения защиты информации в платежной системе Банка России согласно 672-П Порядок защиты информации с помощью СКЗИ в платежной системе Банка России.	3, 5, 6, 7, 8, 32
2	2	5	Внутрирегиональные электронные расчеты Банка России и их безопасность. Межрегиональные электронные расчеты Банка России и их безопасность. Развитие и основные направления трансформации платежной системы Банка России и обеспечения ее безопасности.	3, 5, 6, 7, 8, 12, 13, 32
3	2	6	Тема 3. Прямые межбанковские расчеты и их безопасность. Понятие корреспондентского счета. Виды корреспондентских отношений. Обеспечение безопасности корреспондентского счета.	5, 6, 7, 8, 14, 15, 32
3	2	7	Внутрибанковские расчеты, межфилиальные расчеты и обеспечение их безопасности.	5, 6, 7, 8, 16, 19, 32
3	2	8	Расчеты между банками - корреспондентами и обеспечение их безопасности.	5, 6, 7, 8, 32
4	2	9	Тема 4. Клиринговые расчеты и их безопасность. Организация клиринга в России. Расчетные небанковские кредитные организации (НКО). Организация и технология клиринга. Обеспечение безопасности клиринга.	6, 7, 8, 32
4	2	10	Обеспечение расчетов по итогам клиринга и их безопасность. Межбанковский клиринг. Клиринг при использовании банковских платежных карт. Клиринг на биржевом рынке.	6, 7, 8, 32
5	2	11	Тема 5. Платежные системы с использованием банковских карт и их безопасность.	6, 7, 8, 20, 32
5	2	12	Развитие платежных систем с использованием банковских платежных карт и обеспечение их безопасности	7, 8, 32
5	2	13	Банковские услуги с использованием пластиковых	7, 8, 17, 18, 32

			карт и их безопасность. Общие правила документооборота при расчетах по операциям с использованием банковских карт.	
5	2	14	Технология овердрафтного кредитования с использованием пластиковых карточек и ее безопасность.	7, 8, 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**	Нормативные документы Банка России.	1, 2, 3, 10, 11, 32
1	**2**	**2**	Финансовые технологии совершения безналичных расчетов и их безопасность.	3, 5, 19, 32
2	**2**	**3**	Роль и место Центральных банков в платежных системах зарубежных стран.	2, 7, 8, 14, 32
3	**2**	**4**	Международные расчеты и их безопасность.	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**	Работа электронного бизнеса с применением серверных приложений SQL. Обеспечение безопасности базы данных MySQL.	1, 2, 3, 32
2	8	**2**	Порядок осуществления расчетных операций в платежной системе Банка России	1, 2, 3, 32
2	4	**3**	Система внутрирегиональных расчетов и ее безопасность	3, 5, 32
2	2	**4**	Система межрегиональных расчетов и ее безопасность	5, 6, 32
3	5	**5**	Основные технологии межбанковских электронных расчетов и их безопасность	6, 7, 32
4	4	**6**	Особенности организации системы международных электронных межбанковских расчетов и их безопасность	6, 7, 8, 32
5	6	**7**	Банковские услуги с использованием пластиковых карт и их безопасность.	7, 8, 9, 10, 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	Платежные системы и их развитие в России	2, 4, 5, 10, 12, 18, 19, 20, 21, 22, 29, 30, 31, 32
2	10	Безналичные расчеты в экономике России. Анализ практики.	
3	16	Правила обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России	
4	11	Порядок приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями	
5	14	Управление деятельностью коммерческого банка (банковский менеджмент)	

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

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

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
1	Б.1.3.12.2 Безопасность электронного бизнеса	Знает: - виды и способы дистанционного оказания банковских услуг; - классификацию пластиковых карточек, базовые технологии их использования; - правила, процедуры, практические приемы для управления информационной безопасностью; - требования, методы и средства информационной безопасности в технологиях платежных систем;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - проводить анализ систем электронного бизнеса с точки зрения обеспечения информационной безопасности; - разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы; - реализовывать меры противодействия выявленным угрозам безопасности платежных систем с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения; - составлять комплекс мер для управления информационной безопасностью;	Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - навыками работы с нормативно-правовыми актами и методическими документами; - навыками проектирования защищенных систем	Лекции Практические занятия с использованием активных и интерактивных приемов обучения.	Экзамен

		электронного бизнеса; - навыками комплексного анализа защищенности систем электронного бизнеса; - методами организации и управления деятельностью служб защиты информации на предприятии.	Самостоятельная работа	

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. Правовая база регулирования платежной системы. Нормативные документы Банка России.
2. Особенности реформирования платежной системы. Эволюция расчетной системы России.
3. Банковские технологии совершения безналичных расчетов и их безопасность.
4. Финансовые технологии совершения безналичных расчетов и их безопасность.
5. Структура платежной системы России.
6. Основные принципы обеспечения безопасности платежной системы России.
7. Роль и место Центральных банков в платежных системах зарубежных стран.
8. Основные принципы создания и функционирования электронной системы расчетов Банка России и обеспечения ее безопасности.
9. Порядок осуществления расчетных операций через Банк России и обеспечения их безопасности.
10. Внутрирегиональные электронные расчеты Банка России и их безопасность.
11. Межрегиональные электронные расчеты Банка России и их безопасность.
12. Прямые межбанковские расчеты и их безопасность.
13. Понятие корреспондентского счета. Виды корреспондентских отношений.
14. Обеспечение безопасности корреспондентского счета.
15. Внутрибанковские расчеты, межфилиальные расчеты и обеспечение их безопасности.
16. Расчеты между банками - корреспондентами и обеспечение их безопасности. Международные расчеты и их безопасность.
17. Организация клиринга в России.
18. Организация и технология клиринга. Обеспечение безопасности клиринга.
19. Обеспечение расчетов по итогам клиринга и их безопасность. Межбанковский клиринг.
20. Клиринг при использовании банковских платежных карт.
21. Платежные системы с использованием банковских карт и их безопасность.
22. Развитие платежных систем с использованием банковских платежных карт и обеспечение их безопасности
23. Банковские услуги с использованием пластиковых карт и их безопасность.
24. Общие правила документооборота при расчетах по операциям с использованием банковских карт.
25. Технология овердрафтного кредитования с использованием пластиковых карточек и ее безопасность.

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 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. – 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 направления ИФБС интернет-ресурсов СГТУ имени Гагарина Ю.А.
https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.03.01/B.1.3.11.2/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 ИНЭТМ (Windows, Visual Studio), Ubuntu Linux.
2. Средства разработки программ: Microsoft Visual Studio Express в составе DreamsPark Premium MS ИНПИТ, 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.

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