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.1.3.10.1 Угрозы информационной безопасности автоматизированных систем»

направления подготовки
10.03.01 «Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 16
коллоквиум – 2
практические занятия – 18
самостоятельная работа – 36
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины «Угрозы информационной безопасности автоматизированных систем»: изучение основных понятий, типов и источников угроз информационной безопасности в автоматизированных системах.

Задачи изучения дисциплины:

- формирование у обучаемых целостного представления об источниках угроз информационной безопасности;
- дать представление о видах и возможных методах и путях реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области построения модели угроз информационной безопасности.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Угрозы информационной безопасности автоматизированных систем» относится к числу дисциплин специализации профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Технологии и методы программирования», «Основы информационной безопасности», «Криптографические методы защиты информации», «Сети и системы передачи информации», «Безопасность операционных систем».

Дисциплина «Угрозы информационной безопасности автоматизированных систем» является предшествующей и необходимой для изучения следующих дисциплин специализации: «Создание автоматизированных систем в защищенном исполнении», «Оценка информационной безопасности автоматизированных систем в защищенном исполнении», «Управление информационной безопасностью». Знания и практические навыки, полученные по дисциплине «Угрозы безопасности информации», используются при подготовке выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-5 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7 способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций

ПК-7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

Студент должен знать:

- понятие и принципы разработки модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
- угрозы безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
- методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
- технологии моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
- нормативные правовые акты, руководящие и методические документы, регламентирующие вопросы моделирования и определения актуальности угроз безопасности информации;
- состав и содержание мер по определению угроз безопасности информации в процессе создания и эксплуатации
- автоматизированных систем в защищенном исполнении;

Студент должен уметь:

- разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
- выявлять, классифицировать угрозы безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
- выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
- применять современные технологии моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
- применять нормативные правовые акты, руководящие и методические документы, регламентирующие вопросы моделирования и определения актуальности угроз безопасности информации;

– проводить анализ достаточности мер по определению угроз безопасности информации в процессе создания и эксплуатации автоматизированных систем в защищенном исполнении

Студент должен владеть навыками:

– навыком разработки разрабатывать моделей угроз и моделей нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
– навыком определения угроз безопасности информации, потенциально и/или реально существующие в процессе создания и эксплуатации автоматизированных систем;
– навыком выбора методов и средств для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении с учетом угроз безопасности информации;
– навыком применения современных технологий моделирования угроз безопасности информации при проектировании автоматизированных систем в защищенном исполнении;
– навыком применения нормативных правовых актов, руководящих и методических документов, регламентирующих вопросы моделирования и определения актуальности угроз безопасности информации;
– навыком анализа достаточности мер по определению угроз безопасности информации в процессе создания и эксплуатации автоматизированных систем в защищенном исполнении.

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

№ модуля	№ недели	№ темы	Наименование темы	Часы				
				Всего	Лекции	Коллоквиумы	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
8 семестр								
1	1	1	Введение. Угрозы информационной безопасности: основные термины, понятия, определения.	6	2		2	2
1	3	2	Классификация угроз информационной безопасности	8	2		2	4
1	5	3	Угрозы утечки информации по техническим каналам	8	2		-	6

2	7	4	Угрозы несанкционированного доступа к информации	20	4		6	10
2	11	5	Типовые модели угроз информационной безопасности	16	4		4	8
2	15	6	Методика определения угроз безопасности информации в информационных системах	14	2	2	4	6
Всего				72	16	2	18	36

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	**Введение.** Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Угрозы информационной безопасности: основные термины, понятия, определения.	1,2,3,22
2	2	2	**Классификация угроз информационной безопасности.** Классификация угроз информационной безопасности. Источники угроз несанкционированного доступа в информационной системе.	2,3,4,6,11
3	2	3	**Угрозы утечки информации по техническим каналам.** Угрозы утечки информации по техническим каналам. Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.	1,4,7,9,10
4	4	4,5	**Угрозы несанкционированного доступа к информации.** Угрозы несанкционированного доступа к информации в информационной системе. Характеристика уязвимостей системного и прикладного программного обеспечения информационной системы. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности, реализуемые с использованием протоколов межсетевого взаимодействия. Угрозы программно-математических воздействий. Использование нетрадиционных информационных каналов.	1,4,7,9,10
5	4	6,7	**Типовые модели угроз информационной безопасности.** Типовые модели угроз информационной безопасности для автоматизированных рабочих мест, локальных информационных систем и распределенных информационных систем.	1,4,7,9,10

6	2	8,9	**Методика определения угроз безопасности информации в информационных системах.** Процесс определения угроз безопасности информации в информационной системе. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя).	12,4,7,9,10

6. Содержание коллоквиумов

№ темы	Всего часов	№ лекции	Тема. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
6	2	9	**Методика определения угроз безопасности информации в информационных системах.** Определение актуальных угроз безопасности информации в информационной системе.	1,2,4,7,9,10

7. Перечень практических занятий

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	**2**	**4**	**3**
1,2	4	Средство моделирования угроз «Гриф». Общие принципы работы с программой	12,13
4	2	Анализ рисков ИС на основе модели информационных потоков	12,13
4	2	Построение модели информационной системы на основе модели угроз и уязвимостей. Анализ рисков информационной системы на основе модели угроз и уязвимостей	12,13
4	2	Расчет рисков по угрозам конфиденциальность и целостность. Расчет рисков по угрозе отказ в обслуживании. Задание контрмер	12,13
5	4	Построение модели угроз безопасности распределенной информационной системы, имеющей подключение к сетям связи общего пользования или сетям международного информационного обмена	12,13
6	4	Банк данных угроз безопасности информации ФСТЭК	22

8. Перечень лабораторных работ

Лабораторные занятия 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	2	Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации	1-22
2	4	Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных	1-22
3	6	Классификация технических каналов утечки информации. Технические средства промышленного шпионажа	1-22
4	10	Предотвращение угроз несанкционированного доступа к информации	1-22
5	8	Принципы построения частных моделей угроз	1-22
6	6	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных	1-22

№ 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), зачет
4-6	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	зачет

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Курсовой проект учебным планом не предусмотрен.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Формирование компетенций специализации по дисциплине производится на лабораторных и лекционных занятиях, в рамках выполнения самостоятельной работы; закрепление достигается при проведении промежуточной аттестации и сдаче зачета.

Уровни освоения компетенций

Ступени уровней освоения компетенции	Отличительные признаки
Пороговый (удовлетворительный)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на достаточном уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на достаточном уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на достаточном уровне освоения
Продвинутый (хорошо)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на хорошем уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на достаточном хорошем уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на хорошем уровне освоения
Высокий (отлично)	**Знает:** основные понятия, теоретические положения, методы, средства и технологии в рамках формируемой компетенции на высоком уровне освоения **Умеет:** использовать методы и подходы в рамках формируемой компетенции на высоком уровне освоения **Владеет:** навыками применения методов, средств и инструментов в рамках формируемой компетенции на высоком уровне освоения

Уровень освоения обучающимися дисциплины оценивается по результатам приема зачета.

Результаты зачтено оцениваются «зачтено», «не зачтено».

- оценки "зачтено" заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на достаточном уровне освоения, усвоивший взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявивший творческие способности в понимании, изложении и использовании учебно-программного материала;

- оценки "не зачтено" заслуживает студент, обнаруживший пробелы в знании основного учебно-программного материала, допустивший существенные ошибки в ответах на зачете, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения.

Вопросы для зачета

1. Угрозы информационной безопасности: основные термины, понятия, определения.
2. Классификация угроз информационной безопасности.
3. Источники угроз несанкционированного доступа в информационной системе.
4. Угрозы утечки информации по техническим каналам.
5. Угрозы утечки акустической (речевой) информации.
6. Угрозы утечки видовой информации.
7. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.
8. Угрозы несанкционированного доступа к информации в информационной системе. Характеристика уязвимостей системного и прикладного программного обеспечения информационной системы.
9. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности, реализуемые с использованием протоколов межсетевого взаимодействия.
10. Угрозы программно-математических воздействий.
11. Использование нетрадиционных информационных каналов.
12. Типовые модели угроз информационной безопасности для автоматизированных рабочих мест
13. Типовые модели угроз информационной безопасности для локальных информационных систем
14. Типовые модели угроз информационной безопасности для распределенных информационных систем.
15. Процесс определения угроз безопасности информации в информационной системе. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя).
16. Определение актуальных угроз безопасности информации в информационной системе.

Вопросы для экзамена

Экзамен учебным планом не предусмотрен.

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 решения ситуационных задач, дискуссии.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Куприянов, А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. 22 экз.
2. Милославская Н.Г. Управление рисками информационной безопасности [Электронный ресурс]: учебное пособие/ Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 130 с.— Режим доступа: http://www.iprbookshop.ru/12060.— ЭБС «IPRbooks», по паролю
3. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с.— Режим доступа: http://www.iprbookshop.ru/12014.— ЭБС «IPRbooks», по паролю
4. Пластун, И. Л. Технология построения защищенных автоматизированных систем и сетей : учеб. пособие для студ. спец. 075500, 220400 / И. Л. Пластун ; М-во образования и науки Рос. Федерации, Саратовский гос. техн. ун-т. - Саратов : СГТУ, 2010. - 96 с. 40 экз

Дополнительные издания

5. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/12048.— ЭБС «IPRbooks», по паролю
6. Грушо, А. А. Теоретические основы компьютерной безопасности : учеб. пособие / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : ИЦ "Академия", 2009. - 272 с. 10 экз
7. Девянин, П. Н. Модели безопасности компьютерных систем : учеб. пособие для вузов / П. Н. Девянин. - М. : ИЦ "Академия", 2005. - 144 с. 12 экз
8. 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.
9. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с.— Режим доступа: http://www.iprbookshop.ru/12014.— ЭБС «IPRbooks», по паролю

10.Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - 4-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. 18 экз
11. Шаньгин, В. Ф. Защита компьютерной информации [Электронный ресурс]: эффективные методы и средства : учеб. пособие / В. Ф. Шаньгин. - Электрон. текстовые дан. - М. : Изд-во ДМК Пресс, 2010. - Режим доступа: http://lib.sstu.ru/index.php/elmrazdel/melellib/3321

Методические указания для обучающихся по освоению дисциплины

12. 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. - 1 с. - Режим доступа: http://lib. sstu.ru/books/zak 88_08.pdf.
13. 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.

Периодические издания

14. Вестник СГТУ (http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan)
15. Инновационная деятельность (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/)
16.Информационная безопасность регионов (http://www.seun.ru/content/nauka /5/1/index.php).

Интернет-ресурсы

17. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
18. 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).
19. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
20. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
21. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

22. Весь лекционный материал размещен в электронной форме в ИОС специальности ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А.

16. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий используется типовая лекционная аудитория со стандартным мультимедийным оснащением:

- 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 лабораторных работ и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория кафедры ИБС, оснащенная вычислительной техникой: ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт, с подключением к локальной сети СГТУ имени Гагарина Ю.А. и доступом к сети Интернет.

При проведении лабораторных работ в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционная система: Windows XP/7.
2. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.
3. Система анализа и управления информационными рисками «Гриф 2006».