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.3.2.5 «Комплексное обеспечение информационной безопасности автоматизированных систем»

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

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 6
часов в неделю – 5
всего часов – 216,
в том числе:
лекции – 32
коллоквиумы – 4
лабораторные занятия – 54
самостоятельная работа – 126
курсовая работа – 7 семестр
экзамен – 7 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»: подготовка студентов к деятельности по созданию систем информационной безопасности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, на базе комплексного подхода применения правил, процедур, практических приемов, руководящих принципов, методов, средств обеспечения информационной безопасности.

Задачи изучения дисциплины:

сформировать способность к комплексному применению мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированной системы.

2. Место дисциплины в структуре ООП ВПО

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к числу дисциплин вариативной части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Техническая защита информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Разработка и эксплуатация защищенных автоматизированных систем» .

Знания, умения и навыки, сформированные при изучении дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» необходимы при выполнении выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ПК-3 способность использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4 способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5 способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;
ПК-7 способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
ПК-9 способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;
ПК-25 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
ПК-26 способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
ПК-30 способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;
ПК-32 способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации.

Студент должен знать:
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- требования нормативных правовых актов в области обеспечения информационной автоматизированных систем;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- критерии оценки эффективности средств защиты информационно-технологических ресурсов автоматизированной системы;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- содержание принципа комплексности при применении основных мер по защите информации в автоматизированных системах;
- основные методы управления информационной безопасностью;
- принципы формирования политики информационной безопасности в автоматизированных системах;

Студент должен уметь:

- планировать политику безопасности автоматизированных систем;
- оценивать эффективность применения средств защиты информации;
- эффективно использовать различные методы и средства защиты информации для автоматизированных систем;
- реализовывать политику информационной безопасности автоматизированных систем;
- применять средства обеспечения информационной безопасности;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- применять нормативные правовые документы при построении комплексных систем защиты информации;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по обеспечению комплекса мер защиты информации автоматизированных систем;
- разрабатывать и исследовать аналитические и компьютерные модели подсистем
- безопасности автоматизированных систем;
- администрировать подсистемы информационной безопасности автоматизированных систем;
- исследовать эффективность применяемых средств автоматизации;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;
- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- разрабатывать частные политики информационной безопасности автоматизированных систем;
- контролировать эффективность принятых мер по реализации частных политик
- информационной безопасности автоматизированных систем;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

Студент должен владеть:

- навыками работы с нормативными правовыми актами при комплексном подходе к обеспечению информационной безопасности автоматизированных систем;
- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- навыками разработки политики информационной безопасности автоматизированных систем;
- методами контроля эффективности принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
- навыками управления информационной безопасностью автоматизированных систем.

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	СРС
1	2	3	4	5	6	7	8	9
8 семестр								
1	1	1	Сущность и задачи комплексной защиты информации.	14	2		2	10
1	2		Принципы организации и этапы разработки КСЗИ.	30	6/2		10	14
1	5		Определение и нормативное закрепление состава защищаемой информации.	28	4/2		6	18
1	7		Каналы и методы дестабилизирующего воздействия на информацию.	28	4/2		6	18
2	9		Определение компонентов комплексной системы защиты информации	30	6/2		8	16
2	12		Разработка модели комплексной системы защиты информации.	36	6/4		10	20
2	15		Назначение, структура и содержание управления комплексной системой защиты информации	26	4/2		6	16

2	17		Оценка эффективности комплексной системы защиты информации.	24	-	4/4	6	14
Всего				216	32/14	4/4	54	126

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	**Сущность и задачи комплексной защиты информации.** Понятийный аппарат в области обеспечения безопасности информации. Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации. Цели, задачи и принципы построения комплексной системы защиты информации.	2,3,4,5,21
2	6	2,3,4	**Принципы организации и этапы разработки КСЗИ.** Методологические основы организации комплексной системой защиты информации. Разработка политики безопасности и регламента безопасности предприятия. Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями. Требования, предъявляемые к комплексной системе защиты информации. Требования к организационной и технической составляющим комплексной системы защиты информации. Требования по безопасности, предъявляемые к изделиям ИТ. Этапы разработки комплексной системы защиты информации. Факторы, влияющие на организацию комплексной системы защиты информации.	2,3,4,7,12,21
3	4	5,6	**Определение и нормативное закрепление состава защищаемой информации.** Классификация информации по видам тайны и степеням конфиденциальности. Нормативно-правовые аспекты определения состава защищаемой информации. Определение объектов защиты. Значение носителей защищаемой информации как объектов защиты.	3,4,7,8,11,21
4	4	7,8	**Каналы и методы дестабилизирующего воздействия на информацию**. Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС. Подходы к оценке ущерба от нарушений ИБ. Задачи комплексной системы защиты информации по выявлению угроз и каналов утечки	2,3,4,9,11,21

			информации.	
5	**6**	**9,10,11**	**Определение компонентов комплексной системы защиты информации.** Общее описание архитектуры АС, системы защиты информации и политики безопасности. Формализация описания архитектуры исследуемой АС. Формулирование требований к системе защиты информации. Выбор механизмов и средств защиты информации. Определение важности параметров средств защиты информации. Оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС.	2,3,4,6,21
6	**6**	**12,13,14**	**Разработка модели комплексной системы защиты информации.** Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности и их анализ. Классификация формальных моделей безопасности. Модели обеспечения конфиденциальности. Модели обеспечения целостности. Субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: пример. Описание объекта защиты. Декомпозиция АС на субъекты и объекты. Модель безопасности: неформальное описание. Декомпозиция системы защиты информации. Противостояние угрозам. Реализация системы защиты информации субъекта АС субъектно-объектной модели.	2,3,4,9,10,11,21
7	**4**	**15,16**	**Назначение, структура и содержание управления комплексной системой защиты информации.** Понятие, сущность и цели управления комплексной системой защиты информации. Принципы управления комплексной системой защиты информации. Структура процессов управления. Основные процессы, функции и задачи управления комплексной системой защиты информации. Структура и содержание общей технологии управления комплексной системой защиты информации. Принципы и методы планирования функционирования комплексной системы защиты информации. Виды контроля функционирования комплексной системы защиты информации. Цель проведения контрольных мероприятий в комплексной системе защиты информации. Анализ и использование результатов проведения контрольных мероприятий.	1,2,4,5,11,21

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5
8	2	1	**Оценка эффективности комплексной системы защиты информации.** Общая характеристика подходов к оценке эффективности комплексной системы защиты информации. Вероятностный подход. Оценочный подход. Требования РД СВТ и РД АС. Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408—2002. Экспериментальный подход.	1,2,4,5,11,21
8	2	2	**Оценка эффективности комплексной системы защиты информации.** Методы и модели оценки эффективности КСЗИ. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса.	1,2,4,5,11,21

7. Перечень практических занятий

Практические занятия учебным планом не предусмотрены.

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	4	3
1	2	Выявление факторов, влияющих на организация комплексной системы защиты информации	2,3,4,5,21
2	10	Разработка политики безопасности и регламента безопасности предприятия	2,3,4,7,12,21
3	6	Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих конфиденциальную информацию предприятия, внесение в него изменений и дополнений. Методика выявления состава носителей защищаемой информации.	3,4,7,8,11,21
4	6	Разработка модели угроз и модели нарушителя. Методика выявления нарушителей, тактики их действий и состава интересующей их информации.	2,3,4,9,11,21
5	8	Проектирование системы зашиты информации для существующей АС.	2,3,4,6,21
6	10	Формальное построение модели защиты	2,3,4,9,10,11,21
7	6	Планирование процесса функционирования комплексной системы защиты информации	1,2,4,5,11,21
8	6	Модели оценки эффективности комплексной системы защиты информации	1,2,4,5,11,21

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
2	10	Методология защиты информации. Современный подход	1-21
3	14	Подходы к проектированию систем защиты информации	1-21
3	18	Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав средств обеспечения, подлежащих защите	1-21
4	18	Обеспечение безопасности информации в непредвиденных ситуациях. Реагирование на инциденты информационной безопасности. Резервирование информации и отказоустойчивость	1-21
5	16	Оптимальное построение системы защиты информации.	1-21
6	20	Формализация модели безопасности. Процедура создания пары субъект—объект, наделение их атрибутами безопасности. Осуществление доступа субъекта к объекту. Взаимодействие с внешними сетями. Удаление субъекта—объекта.	1-21
7	16	Аудит информационной безопасности	1-21
8	14	Экономический подход к оценке эффективности комплексной системы защиты информации.	1-21

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

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Задание на курсовую работу включает в себя выполнение исследовательской и проектной части.

12.1. Темы исследовательской части курсового проекта

1. Цели и задачи построения КСЗИ
2. Разработка политики безопасности предприятия
3. Система управления информационной безопасностью предприятия
4. Этапы разработки КСЗИ
5. Исследование факторов, влияющих на организацию КСЗИ
6. Определение объектов защиты на предприятии
7. Методика определения состава защищаемой информации
8. Подходы к оценке ущерба от нарушений ИБ
9. Кадровое обеспечение функционирования КСЗИ
10. Материально-техническое обеспечение КСЗИ
11. Нормативно-методическое обеспечение КСЗИ
12. Планирование функционирования КСЗИ
13. Оценка эффективности КСЗИ
14. Определение источников дестабилизирующего воздействия на информацию
15. Внедрение КСЗИ в организации
16. Аттестация объекта информатизации
17. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы
18. Методы и средства обеспечения информационной безопасности АС
19. Угрозы ИБ АС
20. Методика проведения аудита информационной безопасности на предприятии
21. Программные средства для проведения аудита информационной безопасности на предприятии
22. Управление КСЗИ в условиях чрезвычайных ситуаций
23. Контроль функционирования КСЗИ
24. Особенности работы с персоналом, владеющим конфиденциальной информацией
25. Принципы построения КСЗИ
26. Этапы проектирования КСИБ
27. Инженерно-техническая защита АС предприятия

12.2. Задание практической части курсового проекта содержит разработку системы обеспечения информационной безопасности информационной системы персональных данных.

12. Курсовой проект

Курсовой проект не предусмотрен

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

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

Вопросы для экзамена

1. Цели и задачи защиты информации в автоматизированных системах.
2. Цели, задачи и принципы построения комплексной системы защиты информации.
3. Политика безопасности и регламент безопасности предприятия.
4. Система управления информационной безопасностью предприятия.
5. Требования, предъявляемые к комплексной системе защиты информации.
6. Этапы разработки комплексной системы защиты информации. Факторы, влияющие на организацию комплексной системы защиты информации.
7. Классификация информации по видам тайны и степеням конфиденциальности.
8. Нормативно-правовые аспекты определения состава защищаемой информации.
9. Определение объектов защиты.
10. Факторы, создающие угрозу информационной безопасности.
11. Угрозы безопасности информации.
12. Модели нарушителей безопасности АС.
13. Оценка ущерба от нарушений ИБ.
14. Задачи комплексной системы защиты информации по выявлению угроз и каналов утечки информации.
15. Описание архитектуры АС, системы защиты информации и политики безопасности.
16. Характеристика задач моделирования КСЗИ.
17. Понятие, сущность и цели управления комплексной системой защиты информации.
18. Принципы управления комплексной системой защиты информации. Структура процессов управления.
19. Оценка эффективности комплексной системы защиты информации.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВПО 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 18 часов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный

технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю
2. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 с.— Режим доступа: http://www.iprbookshop.ru/7008.— ЭБС «IPRbooks», по паролю
3. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс]: учебное пособие/ Коваленко Ю.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 140 с.— Режим доступа: http://www.iprbookshop.ru/12026.— ЭБС «IPRbooks», по паролю
4. 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.

Дополнительные издания

5. Братановский С.Н. Специальные правовые режимы информации [Электронный ресурс]: монография/ Братановский С.Н., Лебедева М.М.— Электрон. текстовые данные.— Саратов: Электронно-библиотечная система IPRbooks, 2012.— 170 с.— Режим доступа: http://www.iprbookshop.ru/9010.— ЭБС «IPRbooks», по паролю
6. Ковалева Н.Н. Комментарий к ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]/ Ковалева Н.Н., Холодная Е.В.— Электрон. текстовые данные.— М.: Новая правовая культура, 2008.— 257 с.— Режим доступа: http://www.iprbookshop.ru/1595.— ЭБС «IPRbooks», по паролю
7. 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
8. Некраха А.В. Организация конфиденциального делопроизводства и защита информации [Электронный ресурс]: учебное пособие/ Некраха А.В., Шевцова Г.А.— Электрон. текстовые данные.— М.: Академический Проект, 2015.— 222 с.— Режим доступа: http://www.iprbookshop.ru/36849.— ЭБС «IPRbooks», по паролю
9. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / А. А. Стрельцов [и др.] ; под. ред. А. А. Стрельцова. - М.: ИЦ "Академия", 2008. - 256 с. 9экз
10.Правовое обеспечение информационной безопасности : учеб. пособие / С. Я. Казанцев [и др.] ; под ред. С. Я. Казанцева. - 3-е изд., стер. - М.: ИЦ "Академия", 2008. - 240 с. 10 экз.

11. 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

Периодические издания

12. Вестник СГТУ (http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan)
13. Инновационная деятельность (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/)
14. Журнал «Инновации + Паблисити» (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/)
15. Информационная безопасность регионов (http://www.seun.ru/content/nauka /5/1/index.php).

Интернет-ресурсы

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

Источники ИОС

21. Весь лекционный материал размещен в электронной форме в ИОС направления ИФБС интернет-ресурсов СГТУ имени Гагарина Ю.А.

16. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

– персональный компьютер (в конфигурации не хуже: процессор Intel Core 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);
– проектор (разрешение не менее 1280x1024);
– экран для проектора.

Для проведения лабораторных занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт.