Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.В.ОД.4 Технология построения защищенных автоматизированных систем»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №4 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2020

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 1 от "31" августа 2020 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнители:
Зав. каф. КБМОИС, доцент *должность* *подпись* И.В. Влацкая *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 113123

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

целью дисциплины «Технология построения защищенных автоматизированных систем» является формирование у студентов знаний основ технологии построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

Задачи:

— концепции обеспечения информационной безопасности автоматизированных систем;

— технологии функционирования защищенной автоматизированной системы;

— методологии оценки защищенности автоматизированных систем;

— принципов построения защищенных информационных систем;

— методов и средств проектирования, создания и сопровождения защищенных автоматизированных систем;

— технологического цикла реализации защищенной системы обработки и хранения информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.28 Основы информационной безопасности, С.1.Б.29 Модели безопасности компьютерных систем, С.1.Б.34 Защита программ и данных, С.1.Б.39 Криптографические протоколы, С.1.Б.40 Теоретико-числовые методы в криптографии*

Постреквизиты дисциплины: *С.2.Б.П.3 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: основные модели описания и представления предметной области различных сфер деятельности. **Уметь:** - применять критерии отнесения информации к защищаемой; - классифицировать виды ущерба от НСД. **Владеть:** информацией о системе современного законодательства, регламентирующей вопросы защиты информации и ответственности за нарушение информационной безопасности.	ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности
Знать: - этические нормы программиста; - современные метода и языки программирования. **Уметь:** - анализировать предметную область для решения практической задачи разработки программного обеспечения;	ОК-5 способностью понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- представлять результат анализа предметной области с использованием различных средств. **Владеть:** навыками алгоритмизации и разработки программного кода.	деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать: понятие информации, общую характеристику процессов сбора, передачи, обработки и накопления информации; виды и свойства информации. **Уметь:** - работать с программными средствами общего и специального назначения; - применять типовые технологии реализации методов защиты информации в информационных системах. **Владеть:** навыками применения стандартных программных средств; поиска, сбора, хранения, анализа, преобразования и передачи данных с использованием сетевых компьютерных технологий.	ОПК-7 способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения
Знать: - методы прогнозирования, планирования, выработки решений при различной априорной неопределенности имеющейся информации в соответствии с отечественными и зарубежными стандартами; - способы измерения свойств объектов предметной области в соответствии с отечественными и зарубежными стандартами; - методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации в соответствии с отечественными и зарубежными стандартами; - основные принципы организации информационно-аналитической деятельности в соответствии с отечественными и зарубежными стандартами. **Уметь:** - разрабатывать формализованные модели, методы и алгоритмы решения типовых задач автоматизированной информационно-аналитической поддержки процессов принятия решений в соответствии с отечественными и зарубежными стандартами; - применять методы и средства мониторинга и ситуационного анализа обстановки в соответствии с отечественными и зарубежными стандартами; - использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении задач поддержки процессов принятия решений в соответствии с отечественными и зарубежными стандартами; - оценивать эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации в соответствии с отечественными и зарубежными стандартами **Владеть:** - методологическими основами теории принятия решений, теории измерений, теории прогнозирования и планирования в соответствии с отечественными и зарубежными стандартами;	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- методическими подходами к интерпретации профессионального смысла получаемых результатов анализа информации в соответствии с отечественными и зарубежными стандартами.	
Знать: - основные положения законодательства Российской Федерации в области защиты информации, отечественные и зарубежные стандарты в области информационной безопасности; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - положения стандартов Единой системы конструкторской документации, Единой системы программной документации, основные отечественные и зарубежные стандарты в области информационной безопасности, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем. **Уметь:** применять стандарты в области обеспечения информационной безопасности. **Владеть:** навыками работы с нормативными правовыми актами и стандартами.	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
Знать: современные программные средства разработки проектной и технической документации **Уметь:** изучать и анализировать средства разработки проектной и технической документации **Владеть:** практическими навыками разработки проектной и технической документации	ПК-6 способностью участвовать в разработке проектной и технической документации
Знать: основные угрозы безопасности компьютерных систем; **Уметь:** уметь использовать современные средства защиты компьютерных систем **Владеть:** навыками оценки уровня защищенности компьютерных систем.	ПК-7 способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем
Знать: научно-техническую информации в области требований к уровню защищенности компьютерной системы при аттестации объектов; - Организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации. **Уметь:** - проводить обработку, анализ и систематизацию информации при проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы; - разрабатывать научно-техническую документацию по результатам проведения экспериментально-исследовательских работ при аттестации объектов; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации; - определять класс защищенности автоматизированных систем и ее составных частей; - организовывать экспериментально-исследовательские работы при аттестации объектов с учетом требований к уровню защищенности компьютерной системы;	ПК-9 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- обрабатывать и систематизировать результаты при проведении экспериментально-исследовательских работ при аттестации объектов. **Владеть:** - нормативной базой в области требований к уровню защищенности компьютерной системы.	
Знать: потенциальные угрозы информационной безопасности для конкретного программного средства; **Уметь:** применять современные физические, аппаратные и программные средства защиты информации. **Владеть:** навыками применения и разработки средств управления информационной безопасностью компьютерной системы.	ПК-15 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы
Знать: Основные уязвимости технических средств защиты информации **Уметь:** настраивать и эксплуатировать технические средства защиты информации **Владеть:** навыками работы с современными техническими средствами защиты информации	ПК-19 способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 7 зачетных единиц (252 академических часа).

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**252**	**252**
Контактная работа:	**76,5**	**76,5**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	44	44
Консультации	1	1
Индивидуальная работа и инновационные формы учебных занятий	1	1
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа: *- выполнение курсовой работы (КР);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**175,5** +	**175,5**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Актуальность проблемы обеспечение безопасности автоматизированных информационных систем	14	2		2	10
2	Угрозы информационной безопасности в АС	28	4		4	20
3	Виды мер и основные принципы обеспечения информационной безопасности	26	2		4	20
4	Основные защитные механизмы, используемые в СЗИ	26	2		4	20
5	Организационная структура системы обеспечения информационной безопасности	26	2		4	20
6	Обязанности конечных пользователей и ответственных за ОИБ в подразделениях	14	2		2	10
7	Инструкции по организации парольной и антивирусной защиты	14	2		2	10
8	Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей АС	14	2		2	10
9	Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств АС	14	2		2	10
10	Определение требований к защите ресурсов	16	2		4	10
11	Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач	12	2		2	8
12	Назначение и возможности СЗИ от НДС	16	2		4	10
13	Аппаратные средства СЗИ от НДС	16	2		4	10
14	Проблемы обеспечения безопасности в IP-Сетях	16	2		4	10
	Итого:	252	30		44	178
	Всего:	252	30		44	178

4.2 Содержание разделов дисциплины

1. Актуальность проблемы обеспечение безопасности автоматизированных информационных систем.

Повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности; вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса; концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях; количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам; цель защиты АС и циркулирующей в ней информации.

2. Угрозы информационной безопасности в АС

Особенности современных АС как объектов защиты; уязвимость основных структурно-функциональных узлов, распределенных АС; угрозы безопасности информации, АС и субъектов информационных отношений; источники угроз безопасности; классификация угроз безопасности; преднамеренные и непреднамеренные угрозы; классификация каналов проникновения в систему и утечки информации; неформальная модель нарушителя.

3. Виды мер и основные принципы обеспечения информационной безопасности

Морально-этические, технологические, организационные, меры физической защиты, технические; достоинства и недостатки мер защиты; основные принципы построения защиты ресурсов.

4. Основные защитные механизмы, используемые в СЗИ

Идентификация и аутентификация пользователей; разграничение доступа зарегистрированных пользователей к ресурсам АС; списки полномочий субъектов; списки управления доступом к объекту; атрибутные схемы; регистрация и оперативное оповещение о событиях безопасности; криптографические методы защиты информации; криптографическое сокрытие хранимых и передаваемых по каналам связи данных; контроль целостности и аутентичности передаваемых данных; контроль целостности программных и информационных ресурсов.

5. Организационная структура системы обеспечения информационной безопасности

Цели создания системы обеспечения информационной безопасности; регламентация действий пользователей и обслуживающего персонала АС; понятие технологии обеспечения информационной безопасности; Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты; разовые мероприятия; мероприятия, проводимые по необходимости; служба безопасности; Система организационно-распорядительных документов по организации комплексной системы защиты информации

6. Обязанности конечных пользователей и ответственных за ОИБ в подразделениях

Обязанности ответственного за обеспечение безопасности информации в подразделении; администратор ИБ;

Порядок работы с носителями ключевой информации; обязанности исполнителя; действия при компрометации ключей; ответственность за нарушение.

7. Инструкции по организации парольной и антивирусной защиты

Инструкции по организации парольной защиты; организация антивирусной защиты;

Средства антивирусного контроля.

8. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей АС

Правила именования пользователей; процедура авторизации сотрудников;

9. Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств АС

Обеспечение и контроль физической целостности и неизменности конфигурации аппаратных ресурсов АС; регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов АС; процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций; экстренная модификация (обстоятельства форс-мажор).

10. Определение требований к защите ресурсов

Определение требований к защищенности информации; категорирование защищаемых ресурсов; категории целостности информации; категории конфиденциальности информации; порядок определения категории защищаемых ресурсов.

11. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач

Проектирование и разработка АС; проведение испытаний; эксплуатация; сдача в промышленную эксплуатацию; кризисные ситуации; меры обеспечения непрерывной работы и восстановления работоспособности АС.

12. Назначение и возможности СЗИ НСД

Задачи, решаемые средствами защиты информации от НСД; рекомендации по выбору средств защиты от НСД; показатели защищенности по классам АС; требования руководящих документов Гостехкомиссии РФ к СЗИ от НСД; сертифицированные СЗИ от НСД.

13. Аппаратные средства СЗИ от НСД

Задачи аппаратной защиты; электронный замок «Соболь»; плата Secret Net Card; обеспечение усиленной аутентификации пользователей с применением персональных электронных идентификаторов («таблеток») Touch Memory , Smart -карт и Proximity -карт.

14. Проблемы обеспечения безопасности в IP-Сетях

Типовая корпоративная сеть; угрозы уязвимости и атаки в сетях; классификация уязвимостей; классификация атак; механизмы реализации атак.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Организационные процессы создания автоматизированных систем	4
2	1,2	Проектирование подсистем АС	4
3	1,2	Классификация систем	4
4	3	Модели жизненного цикла автоматизированных систем	4
5	4	Общие принципы проектирования автоматизированных систем в защищенном исполнении	4
6	4,5	Реализация системы управления доступом	4
7	4,5,6	Реализация моделей защиты информации	4
8	7-10	Распределенная АС	2
9	11-13	Программно-аппаратные средства	2
10	11-13	Межсетевые экраны	4
11	11-13	Почтовые протоколы	2
12	13-14	Аттестация автоматизированной системы по требованиям безопасности	2
13	13-14	Разработка документации	4
		Итого:	44

4.4 Курсовая работа (10 семестр)

Темы курсовых работ:

1. Разработка автоматизированной системы проверки почтовых сообщений.
2. Разработка защищенной системы хранения и конвертации документов в различные форматы.
3. Разработка интернет-ресурса профессиональных видеоинструкций.
4. Разработка автоматизированной системы формирования профилей абонентов для интернет-провайдеров.
5. Разработка защищенного облачного хранилища заданий студентов.
6. Разработка автоматизированной системы планирования бюджета.
7. Разработка автоматизированной системы контроля за пассажирским автотранспортом.
8. Разработка защищенной системы автоматизированной актуализации данных персональных контактов.
9. Разработка электронной торговой площадки «ЭТП-Маркет».
10. Разработка автоматизированной системы мониторинга состава транспортных средств.
11. Разработки системы продвижения сайтов на основе статистики поисковых запросов.
12. Разработка автоматизированной системы онлайн тестирование.
13. Разработка виртуального краеведческого музея ОГУ.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учеб. пособие для вузов / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X.

2. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.

5.2 Дополнительная литература

1. Соловьев, Н.А. Системы автоматизации разработки программного обеспечения [Текст] : учеб. пособие / Н. А. Соловьев, Е. Н. Чернопрудова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : Университет, 2012. - 192 с. : ил. - Библиогр.: с. 182-183. - Прил.: с. 184-191. - ISBN 978-5-4417-0086-3.

2. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 413 с. - (Высшее профессиональное образование). - Библиогр.: с. 403-406. - ISBN 978-5-7695-5448-3.

3. Партыка, Т. Л. Информационная безопасность [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной технике / Т. Л. Партыка, И. И. Попов.- 2-е изд., испр. и доп. - Москва : Форум : ИНФРА-М, 2007, 2014. - 368 с. : ил. - (Профессиональное образование). - Библиогр.: с. 343-344. - Глоссарий: с. 406-429. - ISBN 5-91134-095-X. - ISBN 5-16-002849-8.

4. Куприянов, А. И. Основы защиты информации [Текст] : учеб. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов.- 3-е изд., стер. - М. : Академия, 2008. - 254 с. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5761-3.

5. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учеб. пособие для вузов / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с. : ил. - Библиогр.: с. 934-949. - ISBN 5-85438-140-0.

5.3 Периодические издания

1. Информатика и безопасность.
2. Информационная безопасность.
3. Рецензируемый научный журнал «Проблемы информационной безопасности»

5.4 Интернет-ресурсы

− http://www.consultant.ru/ - Информационно-правовая система "КонсультантПлюс";
− http://www.garant.ru/ - Информационно-правовая система "Гарант";
− http://rkn.gov.ru/ - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
− http://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

- Операционная система Windows 7, Windows 10;
- Microsoft Office 2007, Office 2019;
- Microsoft Visual Studio;

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки на базе процессора Intel Core i5;
- системные блоки на базе процессора Intel Pentium Core 2 Duo;
- мониторы моделей Samsung, ViewSonic.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.