Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.2 Технология построения защищенных автоматизированных систем»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.В.2 Технология построения защищенных автоматизированных систем*» рассмотрена и утверждена на заседании кафедры

компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 8 от "25" марта 2024 г.

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

Исполнители:
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 формирования фонда и научной обработки документов
личная подпись Н.Н. Бигалиева *расшифровка подписи*

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

№ регистрации _____

© Влацкая И.В., 2024
© ОГУ, 2024

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 Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.28 Основы информационной безопасности, Б1.Д.Б.29 Модели безопасности компьютерных систем, Б1.Д.Б.34 Защита программ и данных, Б1.Д.Б.39 Криптографические протоколы, Б1.Д.Б.40 Теоретико-числовые методы в криптографии, Б1.Д.Б.42 Стандарты информационной безопасности*

Постреквизиты дисциплины: *Б1.Д.В.7 Разработка мобильных приложений, Б2.П.В.П.2 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта	**Знать:** - способы представления проекта; - этапы процесса организации проектной деятельности; -основные правовые нормы российского законодательства. **Уметь:** - формулировать цели и задачи проекта;

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	- структурировать этапы процесса организации проектной деятельности; - применять элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развиия и обоснования устойчивости проекта. **Владеть:** - навыками использования нормативно-правовых ресурсов в разработке и реализации проектв.
ПК*-2 Формирование требований в защите информации в автоматизированных системах	ПК*-2-В-1 Умеет определять угрозы безопасности информации, обрабатываемой автоматизированной системой ПК*-2-В-2 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации ПК*-2-В-3 Владеет навыками разработки архитектуры системы защиты информации автоматизированной системы	**Знать:** - программно-аппаратные средства защиты компьютерных систем; - программно-аппаратные средства защиты компьютерныхсетей. **Уметь:** - разрабатывать средства защиты информации в компьютерных системах и сетях; -умеет проводить тестирование средств защиты в компьютерных системах и сетях. **Владеть:** - современными методами защиты информации в компьютерных системах и сетях.
ПК*-3 Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	ПК*-3-В-1 Знает основные требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей ПК*-3-В-2 Способен осуществлять разработку и тестирование средств защиты информации компьютерных систем и сетей ПК*-3-В-3 Владеет основными методами защиты информации компьютерных систем и сетей	**Знать:** - современные аппаратные средства защиты информации. **Уметь:** - применять на практике средства аппаратной защиты информации; - разрабатывать собственные программные средства защиты в соответствии с моделью угроз. **Владеть:** - навыками выявления актуальных угроз

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		информационной безопасности и реализации необходимых средств защиты.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**180**	**180**
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;* *- изучение разделов курса в системе электронного обучения* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**103,5** +	**103,5**
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	Автоматизировнные системы. Основные понятия и определения.	20	4		6	10
2	Создание автоматизированных систем в защищенном исполнении (АСЗИ).	34	4		10	20
3	Этапы разработки систем защиты конфиденциальной информации.	32	4		8	20
4	Угрозы информационной безопасности в АС	50	10		10	30
5	Стадии жизненного цикла АС.	44	8		10	26
	Итого:	180	30		44	106
	Всего:	180	30		44	106

4.2 Содержание разделов дисциплины

1. Автоматизировнные системы. Основные понятия и определения.

Автоматизированная и информационная система. Классификация автоматизированных систем. Классы защищенности автоматизированных систем. Стадии разработки АС. Для разработки АС. Нормативная база. Требования к документации.

2. Создание автоматизированных систем в защищенном исполнении (АСЗИ).

Цель создания АСЗИ. Разработка и внедрение АС. ГОСТы на создание и функционирование АСЗИ. Подсистемы АС (аутентификации и авторизации, контроля целостности, межсетевого экранирования, анализа трафика, обнаружения вторжений, антивирусного конторолля, защиты удаленного доступа, подсистемы аудита и дискреционного контроля доступа.

3. Этапы разработки систем защиты конфиденциальной информации.

Формирование требований для системы защиты информации. Проектирование системы защиты информации. Внедрение системы защиты информации. Аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие. Сопровождение системы защиты информации в ходе эксплуатации объекта информатизации. Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении.

4. 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; модель нарушителя, модель угроз по методике ФСТЭК. Определение актуальных угроз. Необходимые средства защиты АС.

5. Стадии жизненного цикла АС.

Гост 34.601. Цель и задачи обеспечения безопасности АС. Техническое задание на разработку АС. Частное техническое задание. Пакет документов по эксплуатации. Программно-аппаратный комплекс. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Система организационно-распорядительных документов по организации комплексной системы защиты информации.

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Организационные процессы создания автоматизированных систем	6
2	1,2	Проектирование АС. Построение структурной схемы АС.	4
3	2,3	Классификация систем. Подсистемы АС в соответствии с Руководящими документами.	6
4	4	Моделирование угроз информационной безопасности АС.	8
5	4,5	Модели жизненного цикла автоматизированных систем	4
6	4,5	Разработка технического задания.	6
7	4,5	Реализация моделей защиты информации	6
8	5	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-Х.

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-Х. - 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. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".
2. Системы безопасности : журнал. - М. : Агентство "Роспечать".
3. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР.

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.

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

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО

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.