Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый Проректор
_____ / С.Н. Щербич /
«30» сентября 2019 г.

Рабочая программа учебной дисциплины

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Направленность: (специализация №7) обеспечение информационной безопасности распределенных информационных систем
Форма обучения: очная

Курган 2019

Рабочая программа дисциплины «Теоретические основы компьютерной безопасности» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения « 29 » августа 2019 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 27 сентября 2019 года, протокол № 2.

Рабочую программу составил:
ст. преподаватель В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Начальник Управления
образовательной деятельности С.Н. Синицын

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		5
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**48**	**48**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	16	16
Самостоятельная работа, всего часов в том числе:	**96**	**96**
Контрольная работа	18	18
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к практическим занятиям, лабораторным работам и рубежному контролю)	51	51
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Теоретические основы компьютерной безопасности» относится к обязательным дисциплинам вариативной части. Блок 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- информатика;
- криптографические методы защиты информации;
- дискретная математика.

Знания и практические навыки, полученные из курса «Теоретические основы компьютерной безопасности», используются студентами при изучении других дисциплин: программно-аппаратные средства защиты информации, организационное и правовое обеспечение информационной безопасности, системы и сети передачи информации, Безопасность сетей ЭВМ, а также при разработке курсовых работ и проектов и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Дисциплина «Теоретические основы компьютерной безопасности» раскрывает основные понятия и формальные модели обеспечения компьютерной безопасности, на базе которых вырабатываются архитектурные, схемотехнические, программно-алгоритмические решения при создании защищенных компьютерных систем, осуществляется анализ состояния безопасности и эффективности функционирования систем защиты информации компьютерных систем.

Целью изучения дисциплины является: освоение принципов и методов защиты информации, комплексного проектирования и анализа защищенных автоматизированных систем (АС).

Задачами дисциплины являются: изучение основ устройства и принципов функционирования АС, методологии проектирования и построения защищенных АС, критериев и методов оценки защищенности АС, средств и методов защиты от несанкционированного доступа (НСД) к информации.

Компетенции, формируемые в результате освоения дисциплины:

— способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

— способность к самоорганизации и самообразованию (ОК-8);

— способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

— способность создавать и исследовать модели автоматизированных систем (ПК-2);

— способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

— способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23).

В результате изучения дисциплины обучающийся должен:

знать:

- угрозы и методы нарушения безопасности АС; (для ОК-8, ПК-23);
- методы и средства реализации защищенных АС; (для ОК-6, ПК-1, ПК-2);
- стандарты по оценке защищенности АС и их теоретические основы (для ОК-6, ПК-6);

уметь:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности; (для ОК-8, ПК-1, ПК-6);
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС (для ОК-6, ПК-2, ПК-6);

иметь навыки:

- навыками построения формальных моделей систем защиты информации АС (для ПК-2, ПК-23);
- навыками использования критериев оценки защищенности АС; (для ПК-2, ПК-6, ПК-23).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер раздела	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
		Семестр 5			
Рубеж 1	I	**СТРУКТУРА ТЕОРИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.**			
		ТЕМА 1. Основные понятия и определения теории компьютерной безопасности.	1		-
		ТЕМА 2. Ценность информации.	1	-	-
		ТЕМА 3. Анализ угроз информационной безопасности.	1	2	-
		ТЕМА 4. Структуризация методов, принципов, и механизмов теории компьютерной безопасности.	1	-	-
		ТЕМА 5. Основные виды атак на АС.	2	-	-
	II	**МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИЩЕННЫХ АС.**			
		ТЕМА 6. Построение систем защиты от угрозы нарушения конфиденциальности информации.	2	2	-
		ТЕМА 7. Построение системы защиты от угрозы нарушения целостности информации.	1	-	-
		ТЕМА 8. Построение системы защиты от угрозы доступности к информации.	1	2	-
		ТЕМА 9. Построение системы защиты от угрозы раскрытия параметров информационной системы.	1	-	-

		ТЕМА 10. Методология обследования и проектирования защиты АС.	2	2	-
Рубеж 2	III	**ПОЛИТИКА БЕЗОПАСНОСТИ**			
		ТЕМА 11. Понятие политики безопасности.	2	-	-
		ТЕМА 12. Модели безопасности на основе дискреционной политики.	2	2	-
		ТЕМА 13. Модели безопасности на основе мандатной (полномочной) политики.	2	-	-
		ТЕМА 14. Модели безопасности на основе тематической политики.	2	2	-
		ТЕМА 15. Модели безопасности на основе ролевой политики.	2	-	-
		ТЕМА 16. Автоматные и теоретико-вероятностные модели невлияния и невыводимости.	2	-	-
		ТЕМА 17. Модели и технологии обеспечения целостности и доступности данных.	1	-	-
		ТЕМА 18. Политика и модели безопасности в распределенных компьютерных системах.	1	2	-
	IV	**ОСНОВНЫЕ КРИТЕРИИ ЗАЩИЩЕННОСТИ АС. КЛАССЫ ЗАЩИЩЕННОСТИ АС.**			
		ТЕМА 19. Основные критерии оценки защищенности АС.	1	-	-
		ТЕМА 20. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).	1	-	-
		ТЕМА 21. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.	1	-	-
		ТЕМА 22. Единые критерии безопасности информационных технологий (Common Criteria).	1	-	-
		ТЕМА 23. Перспективы развития компьютерной безопасности.	1	-	-
		Всего:	**32**	**16**	-

4.2. Содержание лекционных занятий

РАЗДЕЛ I. СТРУКТУРА ТЕОРИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.

Тема 1. Основные понятия и определения теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).

Тема 2. Ценность информации. Модель OSI/ISO. Информационный поток. Аддитивная модель. Порядковая шкала. Решетка ценности.

Тема 3. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

Тема 4. Структуризация методов, принципов, и механизмов теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации.

Тема 5. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.

РАЗДЕЛ II. МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИЩЕННЫХ АС.

Тема 6. Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно-режимные меры защиты. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

Тема 7. Построение системы защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.

Тема 8. Построение системы защиты от угрозы доступности к информации. Эксплуатационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации.

Тема 9. Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.

Тема 10. Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).

РАЗДЕЛ 3. ПОЛИТИКА БЕЗОПАСНОСТИ.

Тема 11. Понятие политики безопасности. Политика (стратегия) безопасности. Формальные модели политик безопасности. Основные типы политики безопасности. Разработка и реализация политики безопасности.

Тема 12. Модели безопасности на основе дискреционной политики. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов.

Тема 13. Модели безопасности на основе мандатной (полномочной) политики. Описание модели Белла-Лападулы (BL). Основная теорема без-

опасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы.

Тема 14. Модели безопасности на основе тематической политики. Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности.

Тематические решетки на основе классификационных множеств. Тематические мультирубрики при мультирубрицированной иерархической классификации субъектов и объектов доступа.

Тема 15. Модели безопасности на основе ролевой политики. Общая характеристика политики ролевого (типизованного) доступа.

Системы с иерархической организацией ролей. Модель индивидуально-группового доступа. MMS-модель Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

Тема 16. Автоматные и теоретико-вероятностные модели невлияния и невыводимости. Понятие и общая характеристика скрытых каналов утечки информации.

Теоретико-вероятностная трактовка автоматной модели Гогена-Мессигера. Технологии представлений (views) в реляционных СУБД как пример реализации подходов информационной невыводимости и информационного невлияния.

Тема 17. Модели и технологии обеспечения целостности и доступности данных. Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных. Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Мандатная модель К. Биба. Уровни целостности данных. Уровни доверия пользователям. Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах.

Тема 18. Политика и модели безопасности в распределенных компьютерных системах. Понятие "распределенность" компьютерных систем в аспекте безопасности.

Дополнительные аспекты политики безопасности в распределенных компьютерных системах. Структура распределенных компьютерных систем в аспекте политики безопасности.

Модель безопасности Варахаратжана. Фазы доступа. Зональная политика безопасности и ее теоретико-множественная формализация (модель).

РАЗДЕЛ 4. ОСНОВНЫЕ КРИТЕРИИ ЗАЩИЩЕННОСТИ АС. КЛАССЫ ЗАЩИЩЕННОСТИ АС.

Тема 19. Основные критерии оценки защищенности АС. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Стандарты по оценке защищенности АС.

Тема 20. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC.

Тема 21. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.

Тема 22. Единые критерии безопасности информационных технологий (Common Criteria). Основные положения «Единых критериев». Требования безопасности. Профили защиты.

Тема 23. Перспективы развития компьютерной безопасности. Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности.

4.3 Практические занятия

Номер раздела	Наименование раздела	Наименование тем практических занятий	Норматив времени, час.
1	***Структура теории компьютерной безопасности***		
	Тема 3. Анализ угроз информационной безопасности.	*Практическая работа №1.* Контроль настроек и работы антивирусных средств.	1
		Практическая работа №2. Изучение настроек и работы файрволов.	1
2	***Методология построения систем защищенных АС***		
	Тема 6. Построение систем защиты от угрозы нарушения конфиденциальности информации.	*Практическая работа №3.* Изучение изолированных программных сред на примере работы с виртуальными машинами.	1
	Тема 8. Построение системы защиты от угрозы доступности к информации.	*Практическая работа №4.* Разработка программы разграничения полномочий пользователей на основе парольной аутентификации	2
	Тема 10. Методология обследования и проектирования защиты АС.	*Практическая работа №5.* Разработка и программная реализация криптографических алгоритмов.	1
	1-ый рубежный контроль	***Тестирование***	***2***
3	***Политика безопасности***		
	Тема 12. Модели безопасности на основе дискреционной политики.	*Практическая работа №6.* Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации	2
	Тема 14. Модели безопасности на основе тематической политики.	*Практическая работа №7.* Использование функций криптографического интерфейса Windows для защиты информации.	1
	Тема 18. Политика и модели безопасности в распределенных компьютерных системах.	*Практическая работа №8.* Реализация атаки типа «троянский конь» в дискреционной модели доступа.	1
	2-ой рубежный контроль	***Тестирование***	***2***
	Итоговое занятие	Защита контрольных работ	2
		Итого:	**16**

4.4 Контрольная работа

Целью контрольной работы является реализация полученных знаний по дисциплине «Теоретические основы компьютерной безопасности». Студент осуществляет выбор темы работы самостоятельно по согласованию с преподавателем. Контрольная работа выполняется в соответствии с индивидуальным заданием. Объем контрольной работы 15- 20 страниц.

К защите работы должны быть представлены:

- действующая программа, реализующая все основные функции, указанные в задании;
- комплект программной и эксплуатационной документации.

ПРИМЕРНАЯ ТЕМАТИКА КОНТРОЛЬНЫХ РАБОТ

I. ТЕОРЕТИЧЕСКИЙ БЛОК

1. Оценка защищенности компьютерной системы университета на основе ОС Windows 7 Professional (NT, 2000, XP) в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) РФ.
2. Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) РФ.
3. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows 7 Professional (NT, 2000, XP) в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) РФ.
4. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) РФ.
5. Оценка защищенности компьютерной системы университета на основе ОС Windows 7 Professional (NT, 2000, XP) в соответствии с требованиями «Оранжевой книги».
6. Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
7. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows 7 Professional (NT, 2000, XP) в соответствии с требованиями «Оранжевой книги».
8. Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
9. Оценка защищенности ОС Windows 7 Professional (NT, 2000, XP) в соответствии со стандартами ISO.
10. Оценка защищенности ОС Linux в соответствии со стандартами ISO.
11. Сравнительный анализ антивирусных пакетов.
12. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.
13. Сравнительный анализ систем обнаружения атак.

14. Сравнительный анализ межсетевых экранов.
15. Оценка защищенности межсетевых экранов компании «Инфотекс» в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) РФ.
16. Сравнение анализаторов безопасности компьютерных систем.
17. Сравнительный анализ средств защиты электронной почты.
18. Анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им.
19. Анализ методов нарушения безопасности сетевых ОС и методов противодействия им.
20. Анализ методов организации антивирусной защиты компьютерных систем.
21. Сравнительный анализ персональных брандмауэров.
22. Анализ средств безопасности в пакете Microsoft Office.
23. Анализ средств защиты от спама.
24. Анализ методов повышения надежности хранения информации на жестких магнитных дисках.
25. Анализ методов обеспечения безопасности электронного магазина.
26. Анализ методов обеспечения безопасности домашней сети.
27. Анализ средств защиты компакт-дисков от несанкционированного копирования.
28. Анализ методов гарантированного удаления конфиденциальной информации на электронных носителях.
29. Разработка лабораторного практикума по изучению подсистемы безопасности ОС Linux.
30. Использование языка сценариев ОС Windows для разграничения прав пользователей компьютерных систем.
31. Разработка макета персонального брандмауэра.
32. Разработка дополнительных средств администрирования ОС Windows 7 Professional (NT, 2000, XP).

II. ПРАКТИЧЕСКИЙ БЛОК

Темы 1-5. Программная реализация криптографической системы ГОСТ 28147-89:

1. Основной шаг криптографического преобразования.
2. Шифрование и расшифрование в режиме простой замены.
3. Шифрование и расшифрование в режиме гаммирования.
4. Шифрование и расшифрование в режиме гаммирования с обратной связью.
5. Генерация и проверка имитовставки (совместно с любым из трех основных режимов).

Примечание: проекты по данным темам должны выполняться и защищаться совместно.

Темы 6-12. Программная реализация криптографических систем DES, 3-DES и DESX:

6 Основная функция шифрования.
7 Шифрование и расшифрование в режиме электронной кодовой книги (ECB).
8 Шифрование и расшифрование в режиме сцепления блоков шифра (CBC).
9 Шифрование и расшифрование в режиме обратной связи по шифротексту (CFB).
10 Шифрование и расшифрование в режиме обратной связи по выходу (OFB).

11 Шифрование и расшифрование по алгоритму 3-DES в одном из режимов.

12 Шифрование и расшифрование по алгоритму DESX в одном из режимов.

Примечание: проекты по данным темам должны выполняться и защищаться совместно.

Темы 13-17. Разработка программы, защищенной от несанкционированного доступа и использующий различные способы аутентификации пользователей:

13 Парольная аутентификация (аналогично лабораторной работе №1) с дополнительными средствами администрирования (задание максимального и минимального сроков действия пароля, ведение списка уже использованных паролей задаваемой максимальной длины и т.д.).

14 Аутентификация пользователей на основе модели «рукопожатия».

15 Аутентификация пользователей по их «росписи» мышью.

16 Аутентификация пользователей по их клавиатурному почерку.

17 Аутентификация пользователей на основе их способности к запоминанию отображаемой на короткое время на экране информации.

Темы 18-22. Разработка программных средств администрирования ОС Windows:

18 Протоколирование в специальном файле событий, связанных с доступом других приложений к выбираемым информационным ресурсам (папкам, принтерам, разделам реестра).

19 Получение списка пользователей, имеющих право доступа к выбираемому информационному ресурсу (файлу, папке, принтеру, разделу реестра), с указанием имеющихся у них прав доступа.

20 Получение списка информационных ресурсов (файлов, папок, разделов реестра) к которым имеет доступ на чтение (запись) задаваемый пользователь.

21 Получение списка папок, к которым имеют право на чтение все пользователи системы.

22 Выявление легко подбираемых паролей пользователей (совпадающих с паролями из специального словаря или не удовлетворяющих задаваемым требованиям сложности).

Примечание: проекты по темам 19-22 выполняются для ОС Windows NT/2000/XP/7 (по темам 19-21 – с файловой системой NTFS).

Темы 23-24. Разработка программных средств защиты от несанкционированного копирования:

23 Сбор, хеширование, вычисление ЭЦП и сохранение ее в реестре, вывод информации о структуре жесткого диска и параметрах BIOS компьютера.

24 Запись (чтение) не копируемой стандартными средствами метки на дискете.

Темы 25-28. Разработка программных средств, выполняющих взаимную аутентификацию (создающих защищенный сеанс связи) двух хостов в сети на основе одного из криптографических протоколов:

25 Трехфазный протокол Microsoft.

26 Протокол CHAP.

27 Протокол S/Key.

28 Протокол SSL/TLS.

Темы 29-32. Разработка программных средств компьютерной стеганографии:

29. Скрытие и извлечение информации в графических файлах.
30. Скрытие и извлечение информации в звуковых файлах.
31. Скрытие и извлечение информации в видеофайлах.
32. Скрытие и извлечение информации в текстовых файлах.

Темы 33-35. Разработка защищенной почтовой клиентской программы:

33. С автоматическим шифрованием (расшифрованием) сообщений и (или) присоединенных к ним файлов.
34. С автоматическим получением ЭЦП под сообщением и (или) присоединенных к нему файлов (при отправке сообщения) и проверкой ЭЦП (при получении сообщения).
35. С автоматической проверкой на вредоносные вложения с помощью одной из программ-сканеров.

Темы 36-37. Разработка программ раскрытия паролей пользователей:

36. Расшифрование паролей пользователей ОС Windows 9x/ME, хранящихся в pwl-файлах.
37. Получение паролей на загрузку ОС, установленных программой BIOS Setup и хранящихся в энергонезависимой (CMOS) памяти компьютера.

Тема 38. Вирусы в макросах документов: способы внедрения, распространения и защиты

- создание вирусов в макросах и их внедрение в различные типы файлов документов (.doc, .xls, .mdb, .htt и др.) с собственными иллюстративными примерами;
- обзор наиболее известных вирусов в макросах документов;
- распространение вирусов в макросах документов (с примерами);
- способы защиты от вирусов в макросах документов (организационные, «ручные», программные).

Тема 39. Программные закладки: типы, способы внедрения и защиты

- определение и классификация программных закладок;
- способы внедрения программных закладок с известными примерами;
- способы взаимодействия между программной закладкой и нарушителем;
- примеры известных программных закладок (BackOrifice, NetBus, DIRT, Paparazzi и др.);
- способы защиты от программных закладок.

Тема 40. Безопасность компьютерных систем на основе инфраструктуры открытых ключей

- назначение и основные понятия инфраструктуры открытых ключей (Public Key Infrastructure);
- компоненты инфраструктуры открытых ключей;
- возможные применения инфраструктуры открытых ключей;
- реализация инфраструктуры открытых ключей в ОС Windows 2000/XP/7;
- другие реализации инфраструктуры открытых ключей;
- демонстрационные примеры использования инфраструктуры открытых ключей.

Темы 41-45. Программная реализация асимметричных криптографических алгоритмов:

41. Шифрование и расшифрование по алгоритму RSA.
42. Генерация сеансового ключа по методу Диффи-Хеллмана.
43. Получение и проверка ЭЦП по алгоритму Эль-Гамаля (ГОСТ Р 34_10-94).
44. Получение и проверка ЭЦП в криптосистеме на основе эллиптических кривых (ГОСТ Р. 34.10-2001).
45. Вычисление функции хеширования по алгоритму ГОСТ Р 34_11-94.

Примечание: проекты по темам 43, 45 и 44, 45 выполняются и защищаются совместно. Выполнение проекта по теме 45 предполагает использование результатов выполнения проектов по темам 1 и 2.

Тема 46. Разработка программных средств администрирования ОС Linux

Одна из тем 19-22, но применительно к ОС Linux.

Тема 47. Программные средства защиты информации для ОС Linux

- оболочки (командные процессоры) с ограничением прав пользователей;
- системные средства шифрования файлов и каталогов;
- дополнительные программные средства шифрования файлов и каталогов;
- программные средства разграничения доступа к объектам на уровне отдельных пользователей;
- примеры использования рассмотренных программных средств.

Тема 48. Средства аудита в операционных системах клона Unix

- аудит в Unix-системах: определение политики аудита, файлы аудита, реакция на события аудита;
- аудит событий безопасности, связанных с доступом к объектам (на примере файлового сервера Samba);
- аудит событий безопасности в коммерческих версиях Unix (Solaris, Unix System V Release 4 и др.);
- сравнение средств аудита в операционных системах Windows и Unix.

Тема 49. Программные средства компьютерной стеганографии

- сущность, применение, методы компьютерной стеганографии, ее отличие от криптографии;
- обзор существующих программных средств компьютерной стеганографии (Contraband, Steganos и др.), их достоинств и недостатков;
- тенденции развития и возможные новые методы компьютерной стеганографии.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале практической работы.

Преподавателем запланировано применение на практических занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим занятиям, к рубежным контролям, выполнение контрольной работы и подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем: - Анализ угроз информационной безопасности - Структуризация методов, принципов, и механизмов теории компьютерной безопасности - Основные виды атак на АС - Методология обследования и проектирования защиты АС - Построение системы защиты от угрозы доступности к информации - Автоматные и теоретико-вероятностные модели невлияния и невыводимости - Модели и технологии обеспечения целостности и доступности данных - Политика и модели безопасности в распределенных компьютерных системах - Основные критерии оценки защищенности АС - Единые критерии безопасности информационных технологий (Common Criteria)	**31** 2 1 2 2 4 4 4 4 4 4
Подготовка к практическим занятиям (по 2часа на каждое занятие)	16
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Контрольная работа	18
Подготовка к экзамену	27
Всего:	**96**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по практическим занятиям.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
5. Контрольная работа.
6. Вопросы к экзамену

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов						
		Вид учебной работы:	Посещение лекций	Выполнение и защита практической работы	Защита контрольной работы	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$1_б$ x16=$16_б$	$5_б$ x 8 =$40_б$	4	5	5	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично						
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы, а также контрольную работу. Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов - 68 для получения оценки «удовлетворительно» «автоматически». По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры.						

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной практической работы (при невозможности дополнительного проведения практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 5 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 20 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%
«удовлетворительно» – 50% - 70%
«хорошо» – 70% - 90%
«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Экзамен проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к экзамену доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и экзамена

1-ый рубежный контроль

1. По каким причинам возникла необходимость в разработке идеологической концепции универсальных правил взаимодействия компьютеров между собой (модель OSI):

а) обеспечение взаимодействия разнородных компьютеров, управляемых различными операционными системами (обеспечение совместимости таких компьютеров при работе в единой сети);

б) неработоспособность прежней реализации глобальной сети Internet;

в) обеспечение контакта между компьютерами и пользователями через реальную и протяженную среду с ее задержками и искажениями.

2. На каком уровне осуществляется активация, поддержка и деактивация передающей среды?

а) на канальном уровне;

б) на физическом уровне;

в) на прикладном уровне;

г) на сеансовом уровне.

3. Сформулируйте аксиому безопасности информации, положенную в основу «Оранжевой Книги».

а) в защищенной КС всегда присутствует активный компонент, выполняющий контроль) операций субъектов над объектами;

б) все вопросы безопасности информации описываются доступами субъектов к объектам;

в) все вопросы безопасности информации описываются доступами объектов к субъектам.

4. В каких состояниях может находиться преобразование информации?

а) существовать;

б) преобразовывать;

в) действовать;

г) храниться.

2-ой рубежный контроль

1. В функции транспортного уровня входит:

а) поддержка интерфейса пользователя;

б) адресация сообщений;

в) восстановление сообщений;

г) организация сеансов связи.

2. В чем заключается преобразование информации?

а) передача информации от одного объекта к другому;

б) отображение слова, описывающее исходные данные в другое слово;

в) удаление информации.

3. Атакой на КС называют:

а) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;

б) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;

в) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4. ***Троянские программы это:***

а) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса;

б) программы, которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям;

в) программы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

Итоговая проверка знаний и навыков по учебной дисциплине «Теоретические основы компьютерной безопасности» проходит в 5-ом семестре - в форме экзамена.

Примерная тематика вопросов, выносимых на экзамен

1. История теории и практики компьютерной безопасности.
2. Структура понятия компьютерная безопасность и основные направления ее обеспечения. Конфиденциальность, целостность и доступность информации.
3. Принципы обеспечения компьютерной безопасности. Систематика методов и механизмов обеспечения компьютерной безопасности.
4. Понятие защищенности (безопасности) компьютерной информации.
5. Модели ценности информации.
6. Понятие угроз безопасности компьютерной информации и их классификация.
7. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99.
8. Человеческий фактор и модель нарушителя безопасности информации.
9. Субъектно-объектная модель компьютерной системы.
10. Понятие потока, доступа и правил разграничения доступа.
11. Основные типы политик разграничения доступа.
12. Монитор безопасности КС и гарантирование выполнение политики безопасности. Изолированная программная среда.
13. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона.
14. Модели безопасности на основе матрицы доступа.
15. Способы организации матрицы доступа и управления доступом в компьютерных системах.
16. Дискреционные модели распространения прав доступа.
17. Модель и теоремы безопасности Харрисона-Руззо-Ульмана. Алгоритмическая неразрешимость проблемы безопасности в модели HRU.
18. Модель типизованной матрицы доступа.
19. Модель TAKE-GRANT.

20. Расширенная модель TAKE-GRANT и анализ путей возникновения информационных каналов.
21. Основы политики мандатного доступа. Решетка безопасности.
22. Модель Белла-ЛаПадулы и основная теорема безопасности.
23. Основные расширения модели Белла-ЛаПадулы.
24. Общая характеристика политики тематического разграничения доступа.
25. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах.
26. Модель тематико-иерархического разграничения доступа
27. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур".
28. Модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями.
29. Политика и зональная модель безопасности в распределенных КС.
30. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.
31. Модели обеспечения целостности. Мандатная модель Кена Биба.
32. Объединение мандатных моделей Белла-Ла Падулы и Кена Биба.
33. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах.
34. Методы и технологии обеспечения доступности (сохранности) данных. Архивирование, журнализация и репликация данных
35. Методы, критерии и шкалы оценки эмпирических объектов. Системы многомерного шкалирования защищенности компьютерных систем.
36. Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.
37. Теоретико-графовые модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности.
38. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа.
39. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Количественные параметры систем индивидуально-группового доступа.
40. Подходы к классификации защищенности операционных систем Unix, Microsoft Windows NT/2000/XP/7 с использованием стандартов TCSEC, руководящих документов Гостехкомиссии РФ и «Единых критериев».
41. Сравнительный анализ стандартов оценки безопасности компьютерных систем TCSEC, руководящих документов Гостехкомиссии РФ и «Единых критериев».

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1 Основная учебная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

2. А.Ю. Щербаков. Современная компьютерная безопасностью. Теоретические основы. Практические аспекты. [Электронный ресурс]: Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - Доступ из ЭБС «Консультант студента».

3. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. – Доступ из ЭБС «Консультант студента».

7.2 Дополнительная учебная литература:

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства. [Электронный ресурс] - Москва : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1. - - Доступ из ЭБС «Консультант студента».

2. Климентьев, К. Е. Компьютерные вирусы и антивирусы : взгляд программиста [Электронный ресурс] - Москва : ДМК Пресс, 2013. - 656 с. - ISBN 978-5-94074-885-4. - Доступ из ЭБС «Консультант студента».

3. Петренко, С. А. Политики безопасности компании при работе в Интернет [Электронный ресурс]. - Москва: ДМК Пресс, 2018. - 397 с. - ISBN 978-5-93700-057-6- Доступ из ЭБС «Консультант студента».

7.3 Методическая литература:

1. Москвин В.В. Методические указания к выполнению лабораторной работы «Разработка программы разграничения полномочий пользователей на основе парольной аутентификации». КГУ, 2015.

2. Москвин В.В. Использование функций криптографического интерфейса windows для защиты информации. КГУ. 2016.

3. Хорев П.Б. Лабораторные работы по курсу «Методы и средства защиты компьютерной информации». Учебное пособие. – М.: Издательство МГТУ «СТАНКИН», 2007.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru.
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;
8. Безопасность - http://groteck.ru/security.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Система KESS поддержки образовательного процесса КГУ http://dist.kgsu.ru/.

Информационно-справочная система «КонсультантПлюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя учебные аудитории и лаборатории, оснащенные современными компьютерами (все – в стандартной комплектации для практических занятий и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет. Обучающимся студентам предоставляется возможность практической работы.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Теоретические основы компьютерной безопасности»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Направленность:
(специализация №7)

Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 4 з.е. (144 академических часа)
Семестр: 5 (очная форма обучения)
Форма промежуточной аттестации: экзамен
Основные разделы дисциплины.

Структура теории компьютерной безопасности. Методология построения систем защищенных АС. Политика безопасности. Основные критерии защищенности АС. Классы защищенности АС.