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

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы бакалавриата

27.03.04 Управление в технических системах
Направленность: системы и технические средства автоматизации и управления
Форма обучения: очная

Курган 2019

Рабочая программа дисциплины «Защита информации в компьютерных системах» составлена в соответствии с учебным планом по программе бакалавриата «Управление в технических системах» (системы и технические средства автоматизации и управления), утвержденной 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

Заведующий кафедрой «АПП»
канд.техн.наук, доцент — Е.К. Карпов

Начальник Управления
образовательной деятельности — С.Н. Синицын

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		3
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	16	16
Практические занятия	-	-
Аудиторные занятия в интерактивной форме, часов	16	16
Самостоятельная работа, всего часов в том числе:	**76**	**76**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	58	58
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение дисциплины базируется на результатах обучения, сформированных при изучении дисциплины «Информационные технологии».

Результаты обучения по дисциплине необходимы для изучения дисциплин «Вычислительные машины, системы и сети», «Информационные сети и телекоммуникации», «Технические средства автоматизации и управления», «Автоматизированные информационно-управляющие системы», «Программное обеспечение систем управления», а также для выполнения разделов курсовых проектов по дисциплинам базовой части и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Защита информации в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно – аппаратных средств.

Задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевого экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Компетенции, формируемые в результате освоения дисциплины:

- способностью производить расчеты и проектирование отдельных блоков и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием (ПК-6);

- готовностью производить инсталляцию и настройку системного, прикладного и инструментального программного обеспечения систем автоматизации и управления (ПК-17).

знать:

– технологии обнаружения компьютерных атак и их возможности (для ПК-17);

– основные уязвимости и типовые атаки на современные компьютерные системы (для ПК-17);

– возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности (для ПК-6, ПК-17);

– методы защиты компьютерных сетей (для ПК-6);

уметь

– выполнять настройку защитных механизмов сетевых программно-аппаратных средств (для ПК-17);

– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей (для ПК-6, ПК-17);

владеть

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации и систем обнаружения компьютерных атак (для ПК-6, ПК-17).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
Рубеж 1	Тема 1	Основные понятия и определения теории компьютерной безопасности	1	-	-
	Тема 2	Структуризация методов, принципов, и механизмов теории компьютерной безопасности	1	-	-
	Тема 3	Методология построения систем защиты информации в компьютерных системах	2	-	4
	Тема 4	Основные виды атак на автоматизированные системы	2	-	5
	Тема 5	Технология межсетевого экранирования	2	-	2
Рубеж 2	Тема 6	Виртуальные частные сети	2	-	5
	Тема 7	Аудит информационной безопасности в компьютерных сетях	2	-	-
	Тема 8	Политики безопасности	2	-	-
	Тема 9	Основные критерии защищенности АС. Классы защищенности АС	2	-	-
		Всего:	**16**	**-**	**16**

4.2. Содержание лекционных занятий

Тема 1. Основные понятия и определения теории компьютерной безопасности.

История развития теории и практики компьютерной безопасности. Информация как объект защиты. Конфиденциальность, целостность и доступность информации. Модели ценности информации. Информационный поток. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).

Угрозы. Классификация угроз безопасности. Модели угроз и модель нарушителя. Утечки информации. Каналы утечек информации. Классификация каналов утечек информации.

Тема 2. Структуризация методов, принципов, и механизмов теории компьютерной безопасности.

Основные направления обеспечения компьютерной безопасности. Основные уровни защиты информации. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.

Тема 3. Методология построения систем защиты информации в компьютерных системах.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров информационной системы: Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации. Стеганографические методы защиты. Контроль целостности информации на МНИ. Цифровая подпись.

Тема 4. Основные виды атак на автоматизированные системы (АС).

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Технологии обнаружения компьютерных атак и их возможности. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

Вредоносное программное обеспечение. Компьютерные вирусы. Классификация вирусов.

Антивирусное программное обеспечение. Классификация антивирусов. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

Тема 5. Технология межсетевого экранирования.

Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.

Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

Тема 6. Виртуальные частные сети.

Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

Защита данных на сетевом уровне. Защищенный обмен электронной почтой.

Тема 7. Аудит информационной безопасности в компьютерных сетях.

Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуни-

кационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.

Тема 8. Политики безопасности

Понятие политики безопасности. Формальные модели политик безопасности. Основные типы политики безопасности. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.

Политика и модели безопасности в распределенных компьютерных системах.

Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.

Тема 9. Основные критерии защищенности АС. Классы защищенности АС.

Основные критерии оценки защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Единые критерии безопасности информационных технологий (Common Criteria).

Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
3	Методология построения систем защиты информации в компьютерных системах	*Лабораторная работа* № 1. Криптографические средства защиты информации: GPG и Truecrypt.	4
4	Основные виды атак на автоматизированные системы	*Лабораторная работа №2.* Контроль настроек и работы антивирусных средств.	4
	1-ый рубежный контроль	***Тестирование***	***1***
5	Технология межсетевого экранирования	*Лабораторная работа №3.* Изучение настроек и работы межсетевых экранов.	2
6	Виртуальные частные сети	*Лабораторная работа №4.* Изучение изолированных программных сред на примере работы с виртуальными машинами.	4
	2-ой рубежный контроль	***Тестирование***	***1***
	Итого		**16**

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 лабораторной работе.

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 лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах 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 лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, к рубежным контролям и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**46**
Основные понятия и определения теории компьютерной безопасности	4
Структуризация методов, принципов, и механизмов теории компьютерной безопасности	3
Методология построения систем защиты информации в компьютерных системах	6
Основные виды атак на автоматизированные системы	6
Технология межсетевого экранирования	6
Виртуальные частные сети	5
Аудит информационной безопасности в компьютерных сетях	6
Политики безопасности	4
Основные критерии защищенности АС. Классы защищенности АС	6
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	8
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**76**

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 лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов, 3 семестр					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$2_б$ х 8= $16_б$	$7_б$ х 4 =$28_б$	13	13	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 (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные работы. Для получения зачета «автоматически» студенту необходимо набрать 61 балл По согласованию с преподавателем студенту могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных 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 (зачету) 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 лабораторных работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной работы (при невозможности дополнительного проведения лабораторной работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной лабораторной работы самостоятельно) – до 7 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 13 вопросов. На каждое тестирование при рубежном контроле студенту отводится 1 академический 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.

Зачет проводится в форме ответа на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету 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 зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и зачета

1-ый рубежный контроль

Вопрос 1. Доступ к информации, не нарушающий правила разграничения доступа, называется…

а) легальным;

б) нелегальным;

в) санкционированным;

г) вредоносным;

д) несанкционированным.

Вопрос 2. Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на множество субъектов, имеющих доступ к данной информации

а) целостность;

б) доступность;

в) конфиденциальность;

г) своевременность.

Вопрос 3. Уязвимость информации — это:

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.

2-ой рубежный контроль

Вопрос 1. К не преднамеренным угрозам относятся:

а) ошибки в разработке программных средств КС;

б) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

в) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

Вопрос 2. . При парольной защите в качестве аутентификационного фактора субъекта выступает

а) то, что он знает;

б) то, чем он владеет;

в) то, что есть часть его самого.

Вопрос 3. Основные направления обеспечения КБ в зависимости от природы средств и методов:

а) компьютерное, криптографическое, бумажное

б) нормативное, формальное, практическое (экспериментальное)

в) нормативно-правовое, инженерно-техническое, организационное, аппаратно-программное

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.
5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.
10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.
11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.
12. Стеганографические методы защиты.
13. Контроль целостности информации на МНИ.
14. Цифровая подпись.
15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.
16. Средства реализации атак.
17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
18. Технологии обнаружения компьютерных атак и их возможности.
19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).
20. Вредоносное программное обеспечение.
21. Компьютерные вирусы. Классификация вирусов.
22. Антивирусное программное обеспечение. Классификация антивирусов.
23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.
24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.
25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
26. Типы межсетевых экранов. Схемы межсетевого экранирования.
27. Фильтрация пакетов. Критерии и правила фильтрации.
28. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика.
29. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

30. Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.
31. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.
32. Защита данных на сетевом уровне. Защищенный обмен электронной почтой.
33. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.
34. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.
35. Определение структуры информационно-телекоммуникационных сетей.
36. Программные средства анализа топологии вычислительной сети.
37. Определение маршрутов прохождения сетевых пакетов.
38. Обнаружение объектов сети. Построение схемы сети.
39. Выявление телекоммуникационного оборудования.
40. Выявление и построение схемы информационных потоков защищаемой информации.
41. Понятие политики безопасности. Основные типы политики безопасности.
42. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.
43. Политика и модели безопасности в распределенных компьютерных системах.
44. Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.
45. Основные критерии оценки защищенности АС.
46. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).
47. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.
48. Единые критерии безопасности информационных технологий (Common Criteria).
49. Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности.

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

Основная литература:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы

компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

2. Галатенко, В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».

3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

4. 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 ЭБС «Консультант студента».

Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций : учебное пособие : для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети : Принципы, технологии, протоколы : учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

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/.

При чтении лекций используются слайдовые презентации.

Программные средства обеспечения учебного процесса включают в себя: базовые (операционные системы (Windows); инструментальные средства программирования) и вспомогательные (программы презентационной графики; текстовые редакторы; графические редакторы).

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. Обучающемуся предоставляется возможность практической работы.

В соответствии с ООП дисциплина поддерживается соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Защита информации в компьютерных системах»

образовательной программы высшего образования –
программы бакалавриата

27.03.04 Управление в технических системах

Направленность: системы и технические средства автоматизации и управления

Трудоемкость дисциплины: 3 з.е. (108 академических часа)

Семестр: 3 (очная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Информация как объект защиты. Информационная безопасность. Аппаратно-программные средства защиты информации. Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации. Защита от несанкционированного доступа. Типовые угрозы информационной безопасности. Технологии обеспечения безопасности в компьютерных сетях.

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

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы бакалавриата

27.03.04 Управление в технических системах

Направленность: системы и технические средства автоматизации и управления
Форма обучения: заочная

Курган 2019

Рабочая программа дисциплины «Защита информации в компьютерных системах» составлена в соответствии с учебным планом по программе бакалавриата «Управление в технических системах» (системы и технические средства автоматизации и управления), утвержденной для заочной 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

Заведующий кафедрой «АПП»
канд.техн.наук, доцент — Е.К. Карпов

Начальник Управления
образовательной деятельности — С.Н. Синицын

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Заочная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	***6***	***6***
Лекции	2	2
Лабораторные работы	4	4
Практические занятия	-	-
Аудиторные занятия в интерактивной форме, часов	-	-
Самостоятельная работа, всего часов в том числе:	**102**	**102**
Подготовка к зачету	18	18
Контрольная работа	66	66
Другие виды самостоятельной работы	18	18
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение дисциплины базируется на результатах обучения средней образовательной школы по дисциплине «Информатика».

Результаты обучения по дисциплине необходимы для изучения дисциплин «Вычислительные машины, системы и сети», «Информационные сети и телекоммуникации», «Технические средства автоматизации и управления», «Автоматизированные информационно-управляющие системы», «Программное обеспечение систем управления», а также для выполнения разделов курсовых проектов по дисциплинам базовой части и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Защита информации в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно – аппаратных средств.

Задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевого экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Компетенции, формируемые в результате освоения дисциплины:

- способностью производить расчеты и проектирование отдельных блоков и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием (ПК-6);

- готовностью производить инсталляцию и настройку системного, прикладного и инструментального программного обеспечения систем автоматизации и управления (ПК-17).

знать:

– технологии обнаружения компьютерных атак и их возможности (для ПК-17);

– основные уязвимости и типовые атаки на современные компьютерные системы (для ПК-17);

– возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности (для ПК-6, ПК-17);

– методы защиты компьютерных сетей (для ПК-6);

уметь

– выполнять настройку защитных механизмов сетевых программно-аппаратных средств (для ПК-17);

– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей (для ПК-6, ПК-17);

владеть

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации и систем обнаружения компьютерных атак (для ПК-6, ПК-17).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Заочная форма обучения

Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
		Лекции	Практич. занятия	Лаборатор. работы
Тема 1	Структуризация методов, принципов, и механизмов теории компьютерной безопасности	0,5	-	-
Тема 2	Методология построения систем защиты информации в компьютерных системах	0,5	-	1
Тема 3	Основные виды атак на автоматизированные системы	0,5	-	1
Тема 4	Технология межсетевого экранирования	0,5	-	1
Тема 5	Виртуальные частные сети		-	1
	ИТОГО:	2	-	4

4.2. Содержание лекционных занятий

Тема 1. Структуризация методов, принципов, и механизмов теории компьютерной безопасности.

Основные направления обеспечения компьютерной безопасности. Основные уровни защиты информации. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.

Тема 2. Методология построения систем защиты информации в компьютерных системах.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров информационной системы: Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации. Стеганографические методы защиты. Контроль целостности информации на МНИ. Цифровая подпись.

Тема 3. Основные виды атак на автоматизированные системы (АС).

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Технологии обнаружения компьютерных атак и их возможности. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

Вредоносное программное обеспечение. Компьютерные вирусы. Классификация вирусов.

Антивирусное программное обеспечение. Классификация антивирусов. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

Тема 4. Технология межсетевого экранирования.

Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.

Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
2	Методология построения систем защиты информации в компьютерных системах	*Лабораторная работа* № 1. Криптографические средства защиты информации: GPG и Truecrypt.	1
3	Основные виды атак на автоматизированные системы	*Лабораторная работа №2.* Контроль настроек и работы антивирусных средств.	1
4	Технология межсетевого экранирования	*Лабораторная работа №3.* Изучение настроек и работы межсетевых экранов.	1
5	Виртуальные частные сети	*Лабораторная работа №4.* Изучение изолированных программных сред на примере работы с виртуальными машинами.	1
	Итого		**4**

4.4 Контрольная работа

Контрольная работа по дисциплине способствует овладению студентами знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств. Студенты выбирают тему контрольной работы из перечня тем, предложенных преподавателем.

Контрольная работа выполняется в соответствии с темой работы. Объем контрольной работы 20-25 страниц. К защите работы должны быть представлена пояснительная записка. Рекомендуемая структура пояснительной записки:

- титульный лист
- информационная часть
- введение
- основная часть

- заключение
- список использованных источников

Примерные темы контрольных работ

1. Угрозы безопасности информационной системе.
2. Организационные и физические меры защиты информации.
3. Биометрические средства ограничения доступа.
4. Пластиковые карты.
5. Кодирование и перекодирование информации.
6. Пароли.
7. Защита документов, подготовленных в текстовом редакторе Ms Word.
8. Защита документов, подготовленных в табличном процессоре Excel.
9. Защита html-документов и веб-сайтов.
10. Защита исполняемых программ.
11. Защита носителей информации.
12. Сетевые атаки и организация защиты в сети.
13. Электронная подпись и защита электронных сделок.
14. Защита персональных данных.
15. Основные приемы безопасной работы на компьютере.

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 лабораторной работе.

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 лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, выполнение контрольной работы и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**58**
Основные понятия и определения теории компьютерной безопасности	6
Структуризация методов, принципов, и механизмов теории компьютерной безопасности	6
Методология построения систем защиты информации в компьютерных системах	6
Основные виды атак на автоматизированные системы	8
Технология межсетевого экранирования	8
Виртуальные частные сети	6
Аудит информационной безопасности в компьютерных сетях	6
Политики безопасности	6
Основные критерии защищенности АС. Классы защищенности АС	6
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	8
Контрольная работа	18
Подготовка к зачету	18
Всего:	**102**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Отчеты студентов по лабораторным работам.
2. Контрольная работа.
3. Вопросы к зачету.

6.2. Процедура оценивания результатов освоения дисциплины

Зачет проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. На подготовку ответа студенту отводится 1 астрономический час.

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

6.3 Примеры оценочных средств для зачета

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.

5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.
10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.
11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.
12. Стеганографические методы защиты.
13. Контроль целостности информации на МНИ.
14. Цифровая подпись.
15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.
16. Средства реализации атак.
17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
18. Технологии обнаружения компьютерных атак и их возможности.
19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ) .
20. Вредоносное программное обеспечение.
21. Компьютерные вирусы. Классификация вирусов.
22. Антивирусное программное обеспечение. Классификация антивирусов.
23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.
24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.
25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
26. Типы межсетевых экранов. Схемы межсетевого экранирования.
27. Фильтрация пакетов. Критерии и правила фильтрации.
28. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика.
29. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.
30. Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN.
31. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.
32. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.
33. Защита данных на сетевом уровне. Защищенный обмен электронной почтой.
34. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

35. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.
36. Определение структуры информационно-телекоммуникационных сетей.
37. Программные средства анализа топологии вычислительной сети.
38. Определение маршрутов прохождения сетевых пакетов.
39. Обнаружение объектов сети. Построение схемы сети.
40. Выявление телекоммуникационного оборудования.
41. Выявление и построение схемы информационных потоков защищаемой информации.
42. Понятие политики безопасности. Основные типы политики безопасности.
43. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.
44. Основные критерии оценки защищенности АС.
45. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).
46. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля 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

Основная литература:

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

2. Галатенко, В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».

3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

4. 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 ЭБС «Консультант студента».

Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций : учебное пособие : для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и ин-

форматика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети : Принципы, технологии, протоколы : учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

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/.

При чтении лекций используются слайдовые презентации.

Программные средства обеспечения учебного процесса включают в себя: базовые (операционные системы (Windows); инструментальные средства программирования) и вспомогательные (программы презентационной графики; текстовые редакторы; графические редакторы).

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. Обучающемуся предоставляется возможность практической работы.

В соответствии с ООП дисциплина поддерживается соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Защита информации в компьютерных системах»

образовательной программы высшего образования –
программы бакалавриата

27.03.04 Управление в технических системах

Направленность: системы и технические средства автоматизации и управления

Трудоемкость дисциплины: 3 з.е. (108 академических часа)

Курс: 2 (заочная форма обучения), 4 семестр

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Информация как объект защиты. Информационная безопасность. Аппаратно-программные средства защиты информации. Критерии оценки безопасности компьютерных систем. Криптографические средства защиты информации. Защита от несанкционированного доступа. Типовые угрозы информационной безопасности. Технологии обеспечения безопасности в компьютерных сетях.