Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ковровская государственная технологическая академия имени В.А. Дегтярева»

УТВЕРЖДАЮ
Декан факультета А и Э
_____ Митрофанов А.А.
"____" _____2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ОД.17 Защита информации

Направление подготовки **09.03.01**
Информатика и вычислительная техника

Квалификация (степень) выпускника **Бакалавр**

Программа подготовки **Академический бакалавриат**

Форма обучения **Очная**

Выпускающая кафедра **ПМ и САПР**

Кафедра-разработчик рабочей программы **ПМ и САПР**

Семестр	Трудоем-кость общая, час.(з.е.)	Контактная работа				СРС, час.	Форма промежу-точной аттестации (экз./зачет)
		Трудоемкость контактной работы, час.	Лекций, час.	Практич. занятий, час.	Лаборат. работ, час.		
7	144 (4)	68	17	17	34	76	Экзамен
Итого	144 (4)	68	17	17	34	76	

Ковров
2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разделы рабочей программы

1. Цели освоения дисциплины
1. Место дисциплины в структуре ООП ВО
2. Структура и содержание дисциплины
3. Формы контроля освоения дисциплины
4. Учебно-методическое и информационное обеспечение дисциплины
5. Материально-техническое обеспечение дисциплины

Приложения к рабочей программе дисциплины

Приложение 1. Аннотация рабочей программы

Приложение 2. Оценочные средства и методики их применения

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника

Программу составил:
Котов В.В., доцент каф. ПМ и САПР

Программа рассмотрена на заседании кафедры ПМ и САПР
Протокол № 4 от " 20 " 05 2016

Зав. кафедрой ПМ и САПР _____ Котов В.В.

Эксперты:

Главный конструктор КСУ – начальник управления
Информационных технологий ОАО «ЗиД» _____ Фриман М.Б.

Начальник расчётно-аналитического центра
ФГУП ГК НПЦ им. М.В. Хруничева, д.т.н., профессор _____ Халатов Е.М.

Программа одобрена на заседании УМК факультета автоматики и электроники

Председатель УМК (А и Э)_____ Чащин Е.А., к.т.н.,доцент

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение следующих результатов образования (РО):

знания:

на уровне представлений: основные стандарты в области инфокоммуникационных технологий; стандарты информационной безопасности; нормативные акты в области ИБ;

на уровне воспроизведения: методы и средства обеспечения информационной безопасности компьютерных систем;

на уровне понимания: теоретические основы построения сетевых протоколов; методы аутентификации и идентификации в КС; достоверная вычислительная база.

умения:

теоретические: использовать знания по архитектуре ОС для грамотного взаимодействия с ними;

практические: управлять уровнем информационной безопасности в ОС Windows в соответствии с заданными требованиями, выполнять резервное копирование данных, осуществлять антивирусную защиту, осуществлять криптографическую защиту данных;

навыки: обеспечение комплексных методов защиты информации.

Перечисленные РО являются основой для формирования следующих компетенций:

общекультурных

ОК-4 – способность использовать основы правовых знаний в различных сферах деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина *«Защита информации»* относится к обязательным дисциплинам вариативной части дисциплин.

Необходимыми условиями для освоения дисциплины являются: знание *основ построения и архитектуры ЭВМ, технологии разработки и отладки алгоритмов*, умения *применять математические методы для решения практических задач, разрабатывать программы на алгоритмических языках высокого уровня*, владение *навыками работы в операционной системе, алгоритмическим языком*.

Содержание дисциплины является логическим продолжением содержания дисциплин *информатика, ЭВМ и периферийные устройства, Сети и телекоммуникации, Администрирование КС, Операционные системы*.

В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в разделе «Цели освоения дисциплины»:

№ п/п	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины
Общекультурные компетенции			
1	ОК-4	Информатика Сети и телекоммуникации Информатика ЭВМ и ПУ Администрирование КС	Выпускная квалификационная работа

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ модуля образовательной программы	№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
			Лекции	Практические занятия	Лабораторные работы	СРС	Всего часов
1	**1**	Основные положения информационной безопасности и защиты информации	2	4	2	3	**11**
2	**2**	Защита от несанкционированного доступа к информации	3	5	2	3	**13**
	3	Криптографическая защита	2		10	3	**15**
	4	Многоуровневая защита компьютерных сетей	3	2	10	4	**19**
3	**5**	Комплексная защита информации.	1	4		3	**8**
	6	Избыточность и резервное копирование	1	2	2	3	**8**
	7	Вредоносные программы, средства защиты	2		4	3	**9**
	8	Стеганографическая защита информации. Защита данных от копирования	2		2	3	**7**
		Выполнение модульного тестирования	1		2		**3**
		Выполнение РПР				15	**15**
	9	Подготовка к экзамену				36	**36**
ИТОГО:			**17**	**17**	**34**	**76**	**144**

3.1. Содержание (дидактика) дисциплины

Раздел 1. Основные положения информационной безопасности и защиты информации
1.1. Введение в дисциплину. Основные понятия и определения. 1.2. Организационные методы защиты информации.
Раздел 2. Защита от несанкционированного доступа к информации
2.1. Политика информационной безопасности. 2.2. Идентификация пользователей в компьютерной системе. 2.3. Средства и методы ограничения доступа к файлам.
Раздел 3. Криптографическая защита
3.1. Основы криптографии. Симметричное шифрование. 3.2. Асимметричное шифрование. Электронная цифровая подпись.
Раздел 4. Многоуровневая защита компьютерных сетей.
4.1. Основы сетевой безопасности. 4.2. Администрирование сетей. 4.3. Обеспечение информационной безопасности в глобальных сетях.
Раздел 5. Комплексная защита информации.
5.1. Построение комплексных систем защиты информации.
Раздел 6. Избыточность и резервное копирование
6.1. Внесение избыточности и резервное копирование данных.
Раздел 7. Вредоносные программы, средства защиты
7.1. Классы вредоносных программы. 7.2. Средства защиты от вредоносных программ.
Раздел 8. Стеганографическая защита информации. Защита данных от копирования
8.1. Стеганографическая защита информации. 8.2. Защита информации от несанкционированного копирования.
Раздел 9. Подготовка к экзамену. Индивидуальная работа со студентами

3.2. Лекции

№ п/п	Номер раздела дисциплины	Объем, часов	Тема лекции
1	1	1	Введение в дисциплину. Основные понятия и определения.
2		1	Организационные методы защиты информации.
3	2	1	Политика информационной безопасности
4		1	Идентификация пользователей в компьютерной системе.
5		1	Средства и методы ограничения доступа к файлам.
6	3	1	Основы криптографии. Симметричное шифрование.
7		1	Асимметричное шифрование. Электронная цифровая подпись.
8	4	1	Основы сетевой безопасности.
9		1	Администрирование сетей.
10		1	Обеспечение информационной безопасности в глобальных сетях.
11	5	1	Построение комплексных систем защиты информации.
12	6	1	Внесение избыточности и резервное копирование данных.
13	7	1	Классы вредоносных программы.
14		1	Средства защиты от вредоносных программ.
15	8	1	Стеганографическая защита информации.
16		1	Защита информации от несанкционированного копирования.
17	8	1	Подготовка к экзамену
Итого:		**17**	

3.3. Лабораторные работы

№ п/п	Номер раздела дисциплины	Наименование лабораторной работы	Наимен. лаборатории	Трудоемк., часов
1	1	Классификации угроз информационной безопасности		2
2	2	Безопасность в Windows XP		2
3	3	Алгоритм симметричного шифрования		4
4		Алгоритм асимметричного шифрования		4
5		Шифрование с открытым ключом.		2
6	4	Управление безопасностью в Windows Server. Создание домена		2
7		Управление безопасностью в Windows Server. Администрирование пользователей		2
8		Управление безопасностью в Windows Server. Настройка параметров безопасности. Групповые политики		4
9		Использование межсетевого экрана для защиты сети		2
10	6	Управление безопасностью в Windows Server. Резервное копирование и восстановление данных в Windows Server		2
11	7	Антивирусная защита компьютерной системы		4
12	8	Стеганографическая защита информации.		2
13	9	Индивидуальная работа со студентами / выполнение модульного тестирования		2
Итого:				**34**

3.3. Практические занятия

№ п/п	Номер раздела дисциплины	Тема практического занятия	Наимен. лаборат.	Трудоемк., часов
1	1	Законодательство в области информационной безопасности		2
2	1	Политики безопасности предприятия (организации)		2
3	4	Сетевые атаки и методы борьбы с ними		2
4	2	Стандартные средства защиты в операционных системах		2
5	5	Обеспечение конфиденциальности при передаче данных по открытым каналам связи		4
6	2	Управление безопасностью в Windows Server		3
7	6	Резервное копирование данных		2
Итого:				**17**

3.4. Самостоятельная работа студента

Раздел дисциплины	№ п/п	Вид СРС	Трудоемкость, часов
Раздел 1	1	Подготовка к лабораторным работам, оформление отчетов	2
	2	Подготовка к модульному тестированию	1
Раздел 2	3	Подготовка к лабораторным работам, оформление отчетов	2
	4	Подготовка к модульному тестированию	1
Раздел 3	5	Подготовка к лабораторным работам, оформление отчетов	2
	6	Подготовка к модульному тестированию	1
Раздел 4	7	Подготовка к лабораторным работам, оформление отчетов	3
	8	Подготовка к модульному тестированию	1
Раздел 5	9	Подготовка к лабораторным работам, оформление отчетов	3
Раздел 6	10	Подготовка к лабораторным работам, оформление отчетов	2
	11	Подготовка к модульному тестированию	1
Раздел 7	12	Подготовка к лабораторным работам, оформление отчетов	2
	13	Подготовка к модульному тестированию	1
Раздел 8	14	Подготовка к лабораторным работам, оформление отчетов	2
	15	Подготовка к модульному тестированию	1
	16	Выполнение РПР	15
	17	Подготовка к экзамену	36
Итого:			**76**

Примечание: в графе «Вид СРС» указываются конкретные виды СРС (подготовка к лабораторным работам и оформление отчетов, выполнение типового расчета, написание реферата, выполнение расчетно-графического или домашнего задания и т.п.), выполняемые студентом по каждому разделу дисциплины.

3.5. Расчетно-практическая работа

В качестве РПР студент должен выполнить работу по заданной преподавателем теме. Работа оформляется в виде рукописи согласно требованиям ГОСТ. В состав работы обязательно входят следующие части:

1. Титульный лист – 1 стр.
2. Оглавление – 1 стр.
3. Задание на работу и введение – 1 стр.
4. Теоретическая часть – 4-5 стр.
5. Практическая часть 5-10 стр.
6. Заключение (выводы о проделанной работе) – 1 стр.
7. Список литературы – 1 стр.

В ходе написания теоретической части необходимо изучить и кратко изложить сведения, связанные с темой работы.

В практической части приводятся описание и результаты работы: экранные копии, листинги программ и т.п. информация, свидетельствующая о выполнении задания.

Дата выдачи — 6 неделя семестра. Срок сдачи — 14 неделя семестра.

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль освоения дисциплины производится в соответствии с Положениями:
- о системе рейтинг-контроля знаний студентов в ФГБОУ ВО «КГТА им. В.А. Дегтярева»;
- об аттестации студентов ФГБОУ ВО «КГТА им. В.А. Дегтярева».

Текущая аттестация *студентов производится в дискретные временные интервалы лектором и преподавателем (ями), ведущими лабораторные работы и практические занятия по дисциплине в следующих формах:*

- *выполнение лабораторных работ;*
- *защита лабораторных работ;*

Рубежная аттестация *студентов производится по окончании модуля в следующих формах:*

- *защита лабораторных работ;*
- *рейтинг-контроль.*
- *защита домашнего задания.*

Промежуточная аттестация *по результатам семестрам по дисциплине проходит в форме экзамена (включает в себя ответ на теоретические вопросы и решение задач).*

Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить РО по данной дисциплине, включены в состав УМК дисциплины и перечислены в Приложении 4.

Критерии оценивания и таблица планирования результатов обучения (аналог карты рейтинг-контроля знаний студента) приведены в Приложениях 4 и 5.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Введение в защиту информации: Учебное пособие для вузов (УМО) / В.Д. Байбурин – М.: Форум, ИНФРА-М, 2004.-128 с.
2. Информационная безопасность компьютерных систем и сетей: Учебное пособие для вузов (МО)- М.: Д «Форум» - ИНФРА-М, 2008.-416 с.
3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов. –М: Научный мир, 2004.
4. Баричев С.Г. и др. Основы современной криптографии : Учебный курс – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2002.-175 с.

б) дополнительная:

1. Расторгуев С.П. Основы информационной безопасности: Учебное пособие для вузов (УМО). – М.: Академия, 2007.-192 с.
2. Кнут Д. Искусство программирования для ЭВМ. Т.2 Получисленные алгоритмы. М.: Мир,1977.
3. Виноградов И.М. Основы теории чисел. М.: Наука, 1972

в) программное обеспечение, Интернет-ресурсы, электронные библиотечные системы:

1. Операционная система (host), текстовый редактор;
2. Виртуальная машина VMWare / Virtualbox;
3. ОС Windows 2003/2008 Server;
4. Kaspersky Anti-Virus;
5. RAD-система по выбору студента.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Лекционные занятия:
    a. комплект электронных презентаций/слайдов,
    b. аудитория, оснащенная презентационной техникой (проектор, экран, компьютер).
2. Лабораторные работы
    a. Лаборатория 806/808, оснащенная ЭВМ с установленными пакетами программного обеспечения (ПО) общего назначения (ОС Windows, текстовый процессор, RAD-система), а также специализированное ПО: (Виртуальная машина, ОС Windows Server, Kaspersky Anti-Virus).
    b. Указания к лабораторным работам,

Приложение 1
к рабочей программе дисциплины
«Защита информации»

Аннотация рабочей программы

Дисциплина «Защита информации» относится к обязательным дисциплинам вариативной части дисциплин подготовки студентов по направлению 09.03.01 – Информатика и вычислительная техника. Дисциплина реализуется на факультете Автоматики и электроники кафедрой ПМ и САПР.

Дисциплина нацелена на формирование общекультурной ОК-4 компетенции выпускника.

Содержание дисциплины охватывает круг вопросов, связанных с *теоретическим изучением и практической реализацией методов и средств защиты информации в компьютерной системе*.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: *лекции, лабораторные работы, самостоятельная работа студента.*

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме *защиты лабораторных работ*, рубежный контроль в форме *рейтинг-контроля* и промежуточный контроль (аттестация) в форме *экзамена*.

Общая трудоемкость освоения дисциплины составляет **4** зачетные единицы, **144** часа. Программой дисциплины предусмотрены лекционные (17 часов), практические (17 часов), лабораторные (34 часа) занятия и 76 часов самостоятельной работы студента.

Приложение 2
к рабочей программе дисциплины
«Защита информации»

ОЦЕНОЧНЫЕ СРЕДСТВА И МЕТОДИКИ ИХ ПРИМЕНЕНИЯ

Фонды оценочных средств

Фонды оценочных средств, позволяющие определить рейтинговую оценку по данной дисциплине, включают в себя:

- шаблоны отчетов по лабораторным работам – 5 шт., размещены в составе УМК дисциплины;
- комплект тестовых заданий по всем разделам – 50 шт., размещены в базе данных кафедры ПМ и САПР;
- комплект билетов и задач к экзамену – 22 билета, в каждом по 2 вопроса и 1 задача.

Критерии оценивания

Приводятся критерии оценивания каждого вида элементов текущего, рубежного и промежуточного контроля (тестирование, выполнение домашних заданий, работа на практических и семинарских занятиях, выполнение лабораторных работ, выполнение контрольных работ, подготовка и защита реферата, курсового проекта и т.д.) с указанием минимума, обеспечивающего положительную оценку РО.

Выполнение модульного контрольного задания (тестирование)

Тестирование в 1 модуле проводится по следующим темам:

1. Основные положения информационной безопасности и защиты информации
2. Защита от несанкционированного доступа к информации
3. Криптографическая защита
4. Многоуровневая защита компьютерных сетей

Тестирование во 2 модуле проводится по следующим темам:

1. Комплексная защита информации
2. Избыточность и резервное копирование
3. Вредоносные программы, средства защиты
4. Стеганографическая защита информации. Защита данных от копирования

Каждая тема оценивается отдельно от 0 до 100 баллов.

Минимальный положительный балл = 70.

Итоговая оценка за модуль является приведенной суммой всех тем (от 0 до 150) с учетом следующего положения:

Для всех тестов происходит пересчет рейтинга теста, полученного в ЦДО, в баллы по следующим критериям:

- рейтинг теста меньше 50% – 0 баллов,
- рейтинг теста 50% – min балл,
- рейтинг теста 100% – max балл,
- рейтинг теста от 50-100% – пересчет по формуле:

```
([рейтинг теста]-50)/50*([max балл]-[min балл])+[min балл].
```

Наименование вида контроля	Критерий оценки	Баллы
1. Посещение лекций	1.1. Посещение всех лекций (допускается пропуск лекционных занятий по уважительной причине)	10
	1.2. Пропуск 2 (1 для второго рейтинг-контроля) лекции без уважительной причины	5
	1.3. Пропуск более 4 (2 для второго рейтинг-контроля) лекций без уважительной причины	0
2. Ведение конспекта лекций	2.1. Имеется полный и аккуратный конспект всех лекций	10
	2.2. В конспекте содержится материал не по всем лекциям, материал изложен с пропусками	5-7
	2.3. Конспект содержит отрывочные записи, выполнен небрежно	3
	2.4. Конспекта лекций нет	0
3. Работа на лекции	3.1. Студент активно принимает участие в лекции, отвечает на заданные вопросы, задает вопросы по теме лекции	5
	3.2. Студент периодически принимает участие в лекции	3
	3.3. Студент не проявляет интереса к лекции, занимается посторонними делами	0
4. Домашняя подготовка к лабораторной работе	4.1. Студент проработал теоретический материал по лабораторной работе, подготовил теоретическое введение к отчету, принес методические материалы и необходимые принадлежности для выполнения работы	20
	4.2. Студент обладает достаточными теоретическими знаниями для выполнения работы, однако не выполнил все условия, предусмотренные в п. 4.1	7-17
	4.3. Студент пришел не подготовленным к работе	0
5. Выполнение лабораторной работы	5.1. Студент правильно выполнил работу в течении отведенного времени	20
	5.2. Студент выполнил работу в течении отведенного времени с некоторыми замечаниями	10-17
	5.3. Студент выполнял работу, однако не смог или не успел завершить ее	5-10
	5.4. Студент не выполнил работу, не проявлял интереса к выполнению поставленного задания	0
6. Качество выполнения отчета по лабораторным работам	6.1. Отчет по лабораторным работам аккуратно оформлен в соответствии с требованиями, представлен в установленные сроки	20
	6.2. Отчет по лабораторным работам выполнен с замечаниями, не полностью соответствует требованиям, представлен не в срок	10-17
	6.3. Отчет выполнен не по всем работам, с существенными недостатками, оформлен небрежно, представлен не в срок	5-10
	6.4. Отчет по лабораторным работам не представлен	0
7. Защита лабораторной работы	7.1. Все лабораторные работы защищены без ошибок, при защите студент продемонстрировал полные теоретические знания и практические навыки	20
	7.2. Лабораторные работы защищены с замечаниями, продемонстрированные теоретические знания и практические навыки не полны	10-17
	7.3. Лабораторные работы защищены с значительными замечаниями, студент затрудняется ответить на большинство теоретических вопросов и выполнить большинство практических заданий	3-7
	7.4. Лабораторные работы не защищены	0