Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

**Пермский национальный исследовательский
политехнический университет**

Электротехнический факультет
Кафедра информационных технологий и автоматизированных систем

УТВЕРЖДАЮ
Проректор по учебной работе
д-р экон. наук, проф.
_____ Н. В. Лобов
"09" 04 2015 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Разработка средств защиты программного обеспечения»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основная образовательная программа подготовки бакалавров
Направление 230100.62 «Информатика и вычислительная техника»

Профиль подготовки бакалавра: «Вычислительные машины, комплексы, системы и сети»

Квалификация (степень) выпускника: бакалавр

Специальное звание выпускника: бакалавр-инженер

Выпускающая кафедра: Информационные технологии и автоматизированные системы

Форма обучения: очная

Курс: 3 **Семестр(-ы):** 6

Трудоёмкость:

Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч

Виды контроля:

Экзамен: -	Дифференцированный зачёт:	**6 семестр**	Курсовой проект: -	Курсовая работа: -

Пермь 2015

Рабочая программа дисциплины «Разработка средств защиты программного обеспечения» разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования, утверждённого приказом Министерства образования и науки Российской Федерации 9 ноября 2009 г. (номер приказа «553») по направлению подготовки 230100.62 «Информатика и вычислительная техника» (квалификация (степень) «бакалавр»);
- компетентностной модели выпускника ООП по направлению подготовки 230100.62 «Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети», утверждённой 24 июня 2013 г. ;
- базового учебного плана очной формы обучения по направлению подготовки 230100.62 «Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети», утверждённого 29 августа 2011 г.

Рабочая программа согласована с рабочими программами дисциплин «Основы автоматизированного управления», «Вычислительные комплексы и системы», «Управление программными проектами», «Защита информации», «Физика», участвующих в формировании компетенций совместно с данной дисциплиной.

Разработчики доцент _____ (подпись) В.Н. Лясин

ассистент _____ (подпись) И.С. Полевщиков

Рецензент канд. техн. наук, доцент _____ (подпись) Р.Т. Мурзакаев

Рабочая программа рассмотрена и одобрена на заседании кафедры информационных технологий и автоматизированных систем 14 сентября 2015 г., протокол № 2.

Заведующий кафедрой информационных технологий и автоматизированных систем, д-р экон. наук, проф. _____ (подпись) Р.А. Файзрахманов

Рабочая программа одобрена учебно-методической комиссией электротехнического факультета «22» 09 2015 г., протокол № 43.

Председатель учебно-методической комиссии электротехнического факультета, канд. техн. наук, проф. _____ (подпись) А.Л. Гольдштейн

СОГЛАСОВАНО

Заведующий выпускающей кафедрой информационных технологий и автоматизированных систем, д-р экон. наук, проф. _____ (подпись) Р.А. Файзрахманов

Начальник управления образовательных программ, канд. техн. наук, доц. _____ (подпись) Д. С. Репецкий

1 Общие положения

1.1 Цель учебной дисциплины

Целью изучения дисциплины является приобретение знаний, умений и навыков в области принципов и методов разработки защищенных программных систем.

В процессе изучения данной дисциплины студент осваивает следующие компетенции:

– способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности (ПК-6).

1.2 Задачи учебной дисциплины

***– Изучение*:**

– правовых основ защиты компьютерной информации;

– математических основ криптографии;

– организационных, технических и программных методов защиты информации в современных компьютерных системах и сетях;

– стандартов, моделей и методов шифрования;

– методов идентификации пользователей;

– основ инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методов передачи конфиденциальной информации по каналам связи;

– методов установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

***– Формирование умений*:**

– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;

– проводить сравнительный анализ, выбирать методы и средства защиты информации;

– оценивать уровень защиты информационных ресурсов в прикладных системах.

– Формирование навыков:

– построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;

– построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации;

– построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи;

– построения программных систем, содержащих алгоритмы хэш-функций;

– построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.

1.3 Предметом освоения дисциплины являются следующие объекты:

– правовые основы защиты компьютерной информации;

– математические основы криптографии;

– организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;

– стандарты, модели и методы шифрования;

– методы идентификации пользователей;

– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методы передачи конфиденциальной информации по каналам связи;

– методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

1.4 Место учебной дисциплины в структуре профессиональной подготовки выпускников.

Дисциплина относится к вариативной части цикла профессиональных дисциплин и является дисциплиной по выбору студента при освоении ООП по направлению 230100.62 «Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети».

В результате изучения дисциплины обучающийся должен освоить части указанных в пункте 1.1 компетенций и демонстрировать следующие результаты:

знать:

– правовые основы защиты компьютерной информации;

– математические основы криптографии;

– организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;

– стандарты, модели и методы шифрования;

– методы идентификации пользователей;

– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методы передачи конфиденциальной информации по каналам связи;

– методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных);

уметь:

– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;

– проводить сравнительный анализ, выбирать методы и средства защиты информации;

– оценивать уровень защиты информационных ресурсов в прикладных системах;

владеть:

– навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;

– навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации;

– навыками построения программных систем, содержащих алгоритмы про-

становки и проверки электронной цифровой подписи;

– навыками построения программных систем, содержащих алгоритмы хэш-функций;

– навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.

В таблице 1.1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1 – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины
Профессиональные компетенции			
ПК-6	способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	«Физика»	«Вычислительные комплексы и системы», «Управление программными проектами», «Защита информации»

2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование частей компетенции ПК-6.

2.1 Дисциплинарная карта компетенции ПК-6.

Код	Формулировка компетенции
ПК-6	способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности

Код	Формулировка дисциплинарной части компетенции
ПК-6. Б3.ДВ1.2	способность обосновывать принимаемые проектные решения в области разработки средств защиты программного обеспечения

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – правовые основы защиты компьютерной информации; – математические основы криптографии; – организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях; – стандарты, модели и методы шифрования; – методы идентификации пользователей; – основы инфраструктуры систем, построенных с использованием публичных и секрет-	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы для текущего и промежуточного контроля.

ных ключей; – методы передачи конфиденциальной информации по каналам связи; – методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).		
В результате освоения компетенции студент умеет: – применять известные методы и средства поддержки информационной безопасности в компьютерных системах; – проводить сравнительный анализ, выбирать методы и средства защиты информации; – оценивать уровень защиты информационных ресурсов в прикладных системах.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам.
В результате освоения компетенции студент владеет: – навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации; – навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации; – навыками построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи; – навыками построения программных систем, содержащих алгоритмы хэш-функций; – навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.	Лабораторные работы.	Типовые задания к лабораторным работам.

3 Структура учебной дисциплины по видам и формам учебной работы

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	
		6 семестр	Всего
1	2	3	4
1	**Аудиторная работа**	**52**	**52**
	-в том числе в интерактивной форме	52	52
	- лекции (Л)	18	18
	-в том числе в интерактивной форме	18	18
	- практические занятия (ПЗ)	-	-
	-в том числе в интерактивной форме	-	-
	- лабораторные работы (ЛР)	34	34
	-в том числе в интерактивной форме	34	34
2	**Контроль самостоятельной работы (КСР)**	**2**	**2**
3	**Самостоятельная работа студентов (СРС)**	**90**	**90**
	- изучение теоретического материала	34	34
	- расчётно-графические работы	-	-
	- курсовой проект	-	-

	- курсовая работа	-	-
	- реферат	-	-
	- подготовка к аудиторным занятиям (лекциям, лабораторным работам)	16	16
	- подготовка отчетов по лабораторным работам	40	40
	- индивидуальные задания	-	-
	- другие виды самостоятельной работы	-	-
4	Итоговая аттестация по дисциплине: **дифференцированный зачет**	-	-
5	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	**144** **4**	**144** **4**

4 Содержание учебной дисциплины

4.1 Модульный тематический план

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Трудоёмкость, ч / ЗЕ
			аудиторная работа				КСР	итоговая аттестация	самостоятельная работа	
			всего	Л	ПЗ	ЛР				
1	2	3	4	5	6	7	8	9	10	11
1	1	1	6	2	-	4	-	-	10	16
		2	6	2	-	4	-	-	10	16
		3	6	2	-	4	-	-	10	16
	Итого по модулю:		**18**	**6**	**-**	**12**	**0,5**	**-**	**30**	**48,5**
2	2	4	6	2	-	4	-	-	10	16
		5	6	2	-	4	-	-	10	16
	Итого по модулю:		**12**	**4**	**-**	**8**	**0,5**	**-**	**20**	**32,5**
3	3	6	6	2	-	4	-	-	10	16
		7	6	2	-	4	-	-	10	16
	Итого по модулю:		**12**	**4**	**-**	**8**	**0,5**	**-**	**20**	**32,5**
4	4	8	7	1	-	6	-	-	10	17
		9	1	1	-	-	-	-	4	5
		10	1	1	-	-	-	-	3	4
		11	1	1	-	-	-	-	3	4
	Итого по модулю:		**10**	**4**	**-**	**6**	**0,5**	**-**	**20**	**30,5**
Итоговая аттестация			-	-	-	-	-	**диф. зачет**	-	-

Всего:	**52**	**18**	**-**	**34**	**2**	**-**	**90**	**144/4**

4.2 Содержание разделов и тем учебной дисциплины

Модуль 1. Раздел 1. Основы информационной безопасности

Л – 6 ч, ЛР – 12 ч, СРС – 18 ч.

Тема 1. Основные понятия и определения в области информационной безопасности.

Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы.

Тема 2. Традиционное шифрование: классические методы. Криптостойкость.

Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернама. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.

Тема 3. Алгоритмы генерации псевдослучайных последовательностей чисел.

Различные способы создания псевдослучайных чисел.

Модуль 2. Раздел 2. Хэш-функции и аутентификация сообщений. Электронная цифровая подпись

Л – 4 ч, ЛР – 8 ч, СРС – 12 ч.

Тема 4. Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411.

Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

Тема 5. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.

Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.

Модуль 3. Раздел 3. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.

Л – 4 ч, ЛР – 8 ч, СРС – 12 ч.

Тема 6. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.

Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный

криптоанализ. Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.

Тема 7. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.

Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Модуль 4. Раздел 4. Асимметричные системы шифрования (системы с открытым ключом). RSA. Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий

Л – 4 ч, ЛР – 6 ч, СРС – 12 ч.

Тема 8. Асимметричные системы шифрования (системы с открытым ключом). RSA.

Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

Тема 9. Криптография с использованием эллиптических кривых.

Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Тема 10. Безопасность современных сетевых технологий. Протоколы аутентификации.

Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.

Тема 11. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.

Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Управление ключами.

4.3 Перечень тем практических занятий

Не предусмотрены.

4.4 Перечень тем лабораторных работ

Таблица 4.2 – Темы лабораторных работ

№ п.п.	Номер темы дисциплины	Наименование тем лабораторных работ
1	1, 2, 3	Шифрование информации методами традиционного шифрования. Генерация псевдослучайных последовательностей чисел в системах защиты информации.
2	4, 5	Исследование хэш-функций и электронной цифровой подписи.
3	6, 7	Исследование американского стандарта шифрования данных DES и отечественного стандарта шифрования данных (ГОСТ 28147-89).
4	6, 7	Исследование симметричного криптографического алгоритма с AES – подобной структурой Rijndael.
5	8	Шифрование и электронная цифровая подпись с помощью алгоритма RSA. Асимметричные криптосистемы.
6	8	Выработка общего секретного ключа по алгоритму Диффи – Хэллмана.

4.5 Виды самостоятельной работы студентов

Таблица 4.3 – Виды самостоятельной работы студентов (СРС)

Номер темы дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	2	3
Тема 1	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 2	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 3	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 4	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 5	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 6	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 7	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 8	Изучение теоретического материала. Подготовка к аудиторным занятиям. Подготовка отчетов по лабораторным работам.	3 2 5
Тема 9	Изучение теоретического материала.	4
Тема 10	Изучение теоретического материала.	3
Тема 11	Изучение теоретического материала.	3
	Итого:	**90/2,5**

4.5.1. Изучение теоретического материала

При подготовке к аудиторным занятиям студенту рекомендуется изучать конспект лекций, дополнять его сведениями из учебной литературы и электронных ресурсов.

На самостоятельное изучение выносятся отдельные вопросы тем:

Тема 1. Основные понятия и определения в области информационной безопасности.

Модели сетевой безопасности и безопасности информационной системы.

Тема 2. Традиционное шифрование: классические методы. Криптостойкость.

Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.

Тема 3. Алгоритмы генерации псевдослучайных последовательностей чисел.

Методы создания псевдослучайных чисел.

Тема 4. Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411.

Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

Тема 5. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410.

Стандарты цифровой подписи ГОСТ 3410 и DSS.

Тема 6. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения.

Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.

Тема 7. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.

Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Тема 8. Асимметричные системы шифрования (системы с открытым ключом). RSA.

Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

Тема 9. Криптография с использованием эллиптических кривых.

Аналог алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Тема 10. Безопасность современных сетевых технологий. Протоколы аутентификации.

Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.

Тема 11. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.

Управление цифровыми сертификатами. Управление ключами.

4.5.2 Курсовой проект (курсовая работа)
Не предусмотрены.

4.5.3. Реферат
Не предусмотрен.

4.5.4. Расчетно-графические работы
Не предусмотрены.

4.5.5.Индивидуальное задание
Не предусмотрены.

5 Образовательные технологии, используемые для формирования компетенций

В процессе изучения данной дисциплины широко используются активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

При проведении лабораторных работ реализован метод обучения действием: определяются проблемные области; формируются группы; каждая лабораторная работа проводится по своему алгоритму. При проведении лабораторных работ преследуются следующие цели: применение знаний отдельных дисциплин для решения проблем; закрепление основ теоретических знаний; развитие творческих навыков.

Используются интерактивные формы контроля самостоятельной работы студентов (компьютерное тестирование).

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль освоения дисциплинарных частей компетенций проводится в форме тестирования для анализа усвоения материала предыдущей темы.

6.2 Промежуточный контроль освоения заданных дисциплинарных частей компетенций

Промежуточный контроль освоения дисциплинарных частей компетенций проводится по окончании модулей дисциплины в следующих формах:

– защита лабораторных работ (модули 1, 2, 3, 4);

– компьютерное тестирование (модули 1, 2, 3, 4).

6.3 Итоговый контроль освоения заданных дисциплинарных частей компетенций

Дифференцированный зачет по дисциплине выставляется по итогам проведенного промежуточного контроля и при выполнении заданий всех лабораторных работ и самостоятельной работы.

Экзамен не предусмотрен.

Фонды оценочных средств, включающие типовые задания к лабораторным работам, тестовые задания, методы оценки и критерии оценивания, перечень контрольных точек и таблицу планирования результатов обучения, позволяющие оценить результаты освоения данной дисциплины, входят в состав УМКД на правах отдельного документа.

6.4 Виды текущего, промежуточного и итогового контроля освоения элементов и частей компетенций

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	**Вид контроля**			
	ТК	**ПК**	**ЛР**	**Диф. зачет**
В результате освоения компетенции студент знает:				
– правовые основы защиты компьютерной информации;	+	+	-	+
– математические основы криптографии;	+	+	-	+
– организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;	+	+	-	+
– стандарты, модели и методы шифрования;	+	+	-	+
– методы идентификации пользователей;	+	+	-	+
– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;	+	+	-	+
– методы передачи конфиденциальной информации по каналам связи;	+	+	-	+
– методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).	+	+	-	+
В результате освоения компетенции студент умеет:				
– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;	-	-	+	+
– проводить сравнительный анализ, выбирать методы и средства защиты информации;	-	-	+	+
– оценивать уровень защиты информационных ресурсов в прикладных системах.	-	-	+	+
В результате освоения компетенции студент владеет:				
– навыками построения программных систем, использующих сер-	-	-	+	+

висы и механизмы безопасности, протоколы аутентификации;				
– навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации;	-	-	+	+
– навыками построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи;	-	-	+	+
– навыками построения программных систем, содержащих алгоритмы хэш-функций;	-	-	+	+
– навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.	-	-	+	+

Примечание:
ТК – текущий контроль знаний по теме в форме тестирования;
ПК – промежуточный контроль знаний по модулю с использованием автоматизированной системы тестирования;
ЛР – выполнение лабораторных работ с подготовкой отчёта (оценка умений и навыков).

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Вид работы	**Распределение часов по учебным неделям**																		**Итого, ч**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Лекции	2	-	2	-	2	-	2	-	2	-	2	-	2	-	2	-	2	-	**18**
Лабораторные работы	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	-	**34**
КСР	-	-	-	-	0,5	-	-	-	-	0,5	-	-	-	0,5	-	-	-	0,5	**2**
Изучение теоретического материала	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	-	**34**
Подготовка к аудиторным занятиям (лекциям, лабораторным работам)	-	2	-	2	-	2	-	2	-	2	-	2	-	2	-	2	-	-	**16**
Подготовка отчетов по лабораторным работам	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4	4	**40**
Модуль:	**М1**					**М2**					**М3**				**М4**				
Контр. тестирование					+					+				+				+	
Дисциплин. контроль																			**Диф. зачет**

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б3.ДВ1.2 Разработка средств защиты программного обеспечения	**Профессиональный цикл**
(индекс и полное название дисциплины)	(цикл дисциплины)

	базовая часть цикла		обязательная
x	вариативная часть цикла	x	по выбору студента

230100.62	Направление «Информатика и вычислительная техника», профиль «Вычислительные машины, комплексы, системы и сети»
(код направления подготовки)	(полные названия направления подготовки и профиля)

ИВТ / ЭВТ	Уровень подготовки:		специалист	Форма обучения:	x	очная
(аббревиатуры направления и профиля)		x	бакалавр			заочная
			магистр			очно-заочная

2011 (год утверждения учебного плана ООП)

Семестр: 6

Количество групп: 1

Количество студентов: 15

Полевщиков И.С. (*фамилия, инициалы преподавателя*)

ассистент кафедры ИТАС (*должность*)

ЭТФ (*факультет*)

ИТАС (*кафедра*)

(342) 239 13 54 (*контактная информация*)

СПИСОК ИЗДАНИЙ

№	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1	2	3
	1 Основная литература	
1	Информационная безопасность и защита информации : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; Под ред. С. А. Клейменова .— Москва : Академия, 2006, 2008, 2009 .— 331 с.	40
2	Базы данных и знаний. Управление базами и защита информации : учебное пособие / Ю. Н. Липин ; Пермский государственный технический университет .— Пермь : Изд-во ПГТУ, 2008 .— 189 с.	50 + ЭБ
	2 Дополнительная литература	
	2.1 Учебные и научные издания	

карта книго-обеспеченности

1	Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков ; Пермский государственный технический университет .— Пермь : Изд-во ПГТУ, 2007 .— 339 с.	100
2	Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш .— 2-е изд .— Москва : РИОР : ИНФРА-М, 2014 .— 255 с	2
2.2 Периодические издания		
	~~Не требуются~~	
2.3 Нормативно-технические издания		
	~~Не требуются~~	
2.4 Официальные издания		
	~~Не требуются~~	
2.5 Электронные информационно-образовательные ресурсы		
1	Электронная библиотека Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. — Электрон. дан. (1 912 записей). — Пермь, 2014-2015. — Режим доступа: http://elib.pstu.ru/. — Загл. с экрана.	
2	Лань [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010-2015. – Режим доступа: http://e.lanbook.com/. – Загл. с экрана.	

Основные данные об обеспеченности на 14 сентября 2015 г.

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н.В. Тюрикова

Текущие данные об обеспеченности на _____

(*дата контроля литературы*)

Основная литература [ ] обеспечена [ ] не обеспечена

Дополнительная литература [ ] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н.В. Тюрикова

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – Программы, используемые для обучения и контроля

№ п/п	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5

1	ЛР	MyTestX	Свободного распространения	Система программ для создания и проведения компьютерного тестирования, сбора и анализа их результатов.

8.3 Аудио- и видео-пособия

Не предусмотрены.

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, м^2	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	2	3	4	5	6
1	Класс компьютерного оборудования	Кафедра ИТАС	229 к.А	72	30

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	Персональные компьютеры	20	Оперативное управление	229 к.А

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

Пермский национальный исследовательский политехнический университет

Электротехнический факультет
(наименование факультета)

кафедра информационных технологий и автоматизированных систем
(наименование кафедры, ведущей дисциплину)

УТВЕРЖДАЮ
Заведующий кафедрой
информационных технологий и
автоматизированных систем
д-р экон. наук, проф.

_____ Р.А. Файзрахманов
Протокол заседания кафедры № 1
«05» сентября 2016 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Разработка средств защиты программного обеспечения»
(наименование дисциплины по учебному плану)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа академического бакалавриата

Направление 09.03.01 «Информатика и вычислительная техника»
(код и наименование)

Профиль подготовки бакалавриата: Вычислительные машины, комплексы, системы и сети
(наименование профиля/маг.программы/специализации)

Квалификация выпускника: бакалавр
(бакалавр / магистр / специалист)

Выпускающая кафедра: Информационные технологии и автоматизированные системы
(наименование кафедры)

Форма обучения: очная

Курс: 3 . **Семестр**: 6

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч

Виды контроля:
Экзамен: **-нет** Диф. зачёт: **-6 сем.** Курсовой проект: **-нет** Курсовая работа: **- нет**

Пермь 2016

Учебно-методический комплекс дисциплины «Разработка средств защиты программного обеспечения» разработан на основании:

- федерального государственного образовательного стандарта высшего образования, утверждённого приказом Министерства образования и науки Российской Федерации «12» января 2016 г. номер приказа «5» по направлению подготовки 09.03.01 «Информатика и вычислительная техника (уровень бакалавриата)»;
- компетентностной модели выпускника ОПОП по направлению подготовки 09.03.01 «Информатика и вычислительная техника (уровень бакалавриата)», профилю «Вычислительные машины, комплексы, системы и сети», утверждённой «24» июня 2013 г. (с изменениями в связи с переходом на ФГОС ВО);
- базового учебного плана очной формы обучения по направлению подготовки 09.03.01 «Информатика и вычислительная техника (уровень бакалавриата)», профилю «Вычислительные машины, комплексы, системы и сети», утверждённого «28» апреля 2016 г.

Рабочая программа согласована с рабочими программами дисциплин «Правоведение», «Компьютерная графика», «Программирование», «Защита информации», «Базы данных», «Основы предпринимательской деятельности», «Информатика 2», «WEB-технологии», участвующих в формировании компетенций совместно с данной дисциплиной.

1 Общие положения

1.1 Цель учебной дисциплины

Целью изучения дисциплины является приобретение знаний, умений и навыков в области принципов и методов разработки защищенных программных систем.

В процессе изучения данной дисциплины студент осваивает следующие компетенции:

– способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);

– способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования (ПК-2).

1.2 Задачи учебной дисциплины

***– Изучение*:**

– правовых основ защиты компьютерной информации;

– математических основ криптографии;

– организационных, технических и программных методов защиты информации в современных компьютерных системах и сетях;

– стандартов, моделей и методов шифрования;

– методов идентификации пользователей;

– основ инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методов передачи конфиденциальной информации по каналам связи;

– методов установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

***– Формирование умений*:**

– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;

– проводить сравнительный анализ, выбирать методы и средства защиты информации;

– оценивать уровень защиты информационных ресурсов в прикладных системах.

– Формирование навыков:

– построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;

– построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации;

– построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи;

– построения программных систем, содержащих алгоритмы хэш-функций;

– построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.

1.3 Предметом освоения дисциплины являются следующие объекты:

– правовые основы защиты компьютерной информации;

– математические основы криптографии;

– организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;

– стандарты, модели и методы шифрования;

– методы идентификации пользователей;

– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методы передачи конфиденциальной информации по каналам связи;

– методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).

1.4 Место учебной дисциплины в структуре образовательной программы.

Дисциплина относится к вариативной части Блока 1. Дисциплины (модули) и является дисциплиной по выбору при освоении ОПОП по направлению 09.03.01 «Информатика и вычислительная техника (уровень бакалавриата)», профилю «Вычислительные машины, комплексы, системы и сети».

В результате изучения дисциплины обучающийся должен освоить части указанных в пункте 1.1 компетенций и демонстрировать следующие результаты:

знать:

– правовые основы защиты компьютерной информации;

– математические основы криптографии;

– организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях;

– стандарты, модели и методы шифрования;

– методы идентификации пользователей;

– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;

– методы передачи конфиденциальной информации по каналам связи;

– методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных);

уметь:

– применять известные методы и средства поддержки информационной безопасности в компьютерных системах;

– проводить сравнительный анализ, выбирать методы и средства защиты информации;

– оценивать уровень защиты информационных ресурсов в прикладных системах;

владеть:

– навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;

– навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации;

– навыками построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи;

– навыками построения программных систем, содержащих алгоритмы хэш-функций;

– навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.

В таблице 1.1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1 – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины
Общекультурные компетенции			
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	-	«Правоведение» «Защита информации»
Профессиональные компетенции			
ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	«Программирование», «Информатика 2»	«Базы данных», «WEB-технологии»

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Учебная дисциплина обеспечивает формирование частей компетенций ОК-4, ПК-2.

2.1 Дисциплинарная карта компетенции ОК-4

Код	Формулировка компетенции
ОК-4	способность использовать основы правовых знаний в различных сферах деятельности

Код	Формулировка дисциплинарной части компетенции
ОК-4.Б1.ДВ.06.2	способность использовать основы правовых знаний в области разработки средств защиты программного обеспечения в профессиональной деятельности

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – правовые основы защиты компьютерной информации; – организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях; – стандарты, модели и методы шифрования.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы для текущего и промежуточного контроля.
В результате освоения компетенции студент умеет: – проводить сравнительный анализ, выбирать методы и средства защиты информации.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам.
В результате освоения компетенции студент владеет: – навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации; – навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам.

2.2 Дисциплинарная карта компетенции ПК-2

Код	Формулировка компетенции
ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования

Код	Формулировка дисциплинарной части компетенции
ПК-2.Б1.ДВ.06.2	способность разрабатывать защищенные программные системы, используя современные инструментальные средства и технологии программирования

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – математические основы криптографии; – методы идентификации пользователей;	Лекции. Самостоятельная работа студентов по изучению	Тестовые вопросы для текущего и промежуточного контроля.

– основы инфраструктуры систем, построенных с использованием публичных и секретных ключей; – методы передачи конфиденциальной информации по каналам связи; – методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных).	теоретического материала.	
В результате освоения компетенции студент умеет: – применять известные методы и средства поддержки информационной безопасности в компьютерных системах; – оценивать уровень защиты информационных ресурсов в прикладных системах.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам.
В результате освоения компетенции студент владеет: – навыками построения программных систем, содержащих алгоритмы простановки и проверки электронной цифровой подписи; – навыками построения программных систем, содержащих алгоритмы хэш-функций; – навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам.

3 Структура учебной дисциплины по видам и формам учебной работы

Объем дисциплины в зачетных единицах составляет 4 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	
		6 семестр	Всего
1	2	3	4
1	**Аудиторная работа (контактная работа)**	**52**	**52**
	-в том числе в интерактивной форме	52	52
	- лекции (Л)	18	18
	-в том числе в интерактивной форме	18	18
	- практические занятия (ПЗ)	-	-
	-в том числе в интерактивной форме	-	-
	- лабораторные работы (ЛР)	34	34
	-в том числе в интерактивной форме	34	34
2	**Контроль самостоятельной работы (КСР)**	**2**	**2**
3	**Самостоятельная работа студентов(СРС)**	**90**	**90**
	- изучение теоретического материала	34	34
	- расчётно-графические работы	-	-

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1	Содержание стр. 1, 2, 3, 4, 5, 6 изложить в редакции, приведенной на стр. 1а, 2а, 3а, 4а, 5а, 6а соответственно.	Протокол заседания кафедры №1 от «05» сентября 2016 г. Зав. кафедрой информационных технологий и автоматизированных систем д-р экон. наук, проф. Р.А. Файзрахманов
	В табл. 3.1. строку п.4 «Итоговая аттестация по дисциплине: дифференцированный зачет» изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине: дифференцированный зачет».	
	В табл. 4.1.: а) заголовок столбца «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»; б) в столбце 9 заменить слово «аттестация» на «контроль»; в) в предпоследней строке заменить слова «Итоговая аттестация» на «Промежуточная аттестация».	
	П.4.5 «Виды самостоятельной работы студентов» считать п.5 с наименованием «Методические указания для обучающихся по изучению дисциплины».	
	После п.5 дополнить словами: «При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации: 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по лабораторным работам. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п.7. 5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции».	
	Табл. 4.3 «Виды самостоятельной работы студентов (СРС)» считать табл. 5.1.	
	П.4.5.1 «Изучение теоретического материала» считать п.5.1; п.4.5.2 «Курсовой проект (курсовая работа)» считать п.5.2; п.4.5.3 «Реферат» считать п.5.3; п.4.5.4 «Расчётно-графические работы» считать п.5.4; п.4.5.5 «Индивидуальное задание» считать п.5.5; п.5 «Образовательные технологии, используемые для формирования компетенций» считать п.5.6.	
	Наименование раздела 6 «Управление и контроль освоения компетенций» изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	В последнем абзаце п.6.3 слова «входят в состав УМКД на	

	правах отдельного документа» заменить на слова «входят в состав РПД в виде приложения».	
	Наименование раздела 8 «Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».	
	Заменить в тексте раздела 8: - индекс дисциплины «Б3.ДВ1.2» на «Б1.ДВ.06.2»; - слова «Профессиональный цикл» на «Блок 1. Дисциплины (модули)»; - код направления «230100.62» на «09.03.01».	
	Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Наименование п.2.5 «Электронные информационно-образовательные ресурсы» изменить на «Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	В первой («Электронная библиотека…») и второй строке («Лань…») пункта п.2.5 таблицы удалить число 2015.	
	Дополнить п.2.5 таблицы строкой: **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992–. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать разделом 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».	
	После раздела 8.3 «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине» включить подраздел 8.3.1 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».	
	Раздел 8.3 «Аудио- и видео-пособия» считать подразделом 8.3.2 с прежним названием.	
	Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».	