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.т.н., проф.
_____ Н. В. Лобов
«10» _____ 2015 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Защита информации»

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: 4 **Семестр(-ы)**: 7

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

Виды контроля:
Экзамен: **7 семестр** Зачёт: - Курсовой проект: - Курсовая работа: -

Пермь, 2015

Рабочая программа дисциплины «Защита информации» 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 бакалавра 230100.62 «Информатика и вычислительная техника»;
- 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 «Физика», «Управление программными проектами», «Основы автоматизированного управления», «Вычислительные комплексы и системы», «Разработка средств защиты программного обеспечения», участвующих в формировании компетенций совместно с данной дисциплиной.

Разработчики ассистент _____ А.С. Мехоношин

канд. техн. наук, доцент _____ Р.Т. Мурзакаев

Рецензент доцент _____ В.Н. Лясин

Рабочая программа рассмотрена и одобрена на заседании кафедры информационных технологий и автоматизированных систем 3 июня 2015 г., протокол №13.

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

(подпись)

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

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

(подпись)

СОГЛАСОВАНО

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

(подпись)

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

(подпись)

1 Общие положения

1.1 Цель учебной дисциплины

Целью изучения дисциплины является получение знаний в области теоретических основ защиты информации и практических навыков обеспечения защиты программного обеспечения.

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*** основных методов и средств защиты информации.

– ***Формирование умений*** в области технологии защиты программного обеспечения;

– ***Формирование навыков***, необходимых для разработки средств защиты программного обеспечения.

1.3 Предметом освоения дисциплины являются следующие объекты:

– основные типы угроз;
– основные способы защиты от угроз;
– технические средства защиты;
– организационные и юридические средства защиты;
– основы разработки средств защиты.

1.4 Место учебной дисциплины в структуре профессиональной подготовки выпускников.

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

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

Знать:

– основные понятия и направления в защите программного обеспечения;
– источники, риски, формы атак на информацию;
– основные стандарты оценивания защищенности;
– средства и методы предотвращения вторжений;
– основные уязвимости программного обеспечения.

Уметь:

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;
– использовать парольные системы аутентификации;

– инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;

– анализировать регламентирующие документы в области информационной безопасности;

– устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.

Владеть:

– навыками анализа информационной безопасности;

– навыками администрирования безопасности программного обеспечения;

– навыками шифрования информации;

– навыками обеспечения безопасности данных в ОС Windows;

– навыками выявления и устранения уязвимостей программного обеспечения.

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», «Основы автоматизированного управления», «Разработка средств защиты программного обеспечения»	-

2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование части 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.Б.7	способность обосновывать принимаемые проектные решения в области организации защиты информации различных программно-аппаратных комплексов

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – основные понятия и направления в защите программного обеспечения; – источники, риски, формы атак на информацию; – основные стандарты оценивания защищенности; – средства и методы предотвращения вторжений; – основные уязвимости программного обеспечения.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Вопросы к контрольным работам. Вопросы к экзамену.
В результате освоения компетенции студент умеет: – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты; – использовать парольные системы аутентификации; – инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; – анализировать регламентирующие документы в области информационной безопасности; – устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.	Лабораторные работы. Самостоятельная работа студентов.	Типовые задания к лабораторным работам. Задания к экзамену.
В результате освоения компетенции студент владеет: – навыками анализа информационной безопасности; – навыками администрирования безопасности программного обеспечения; – навыками шифрования информации; – навыками обеспечения безопасности данных в ОС Windows; – навыками выявления и устранения уязвимостей программного обеспечения.	Лабораторные работы. Самостоятельная работа студентов (подготовка к лабораторным работам).	Типовые задания к лабораторным работам. Задания к экзамену.

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	
		7 семестр	всего
1	2	3	4
1	**Аудиторная работа**	**50**	**50**
	-в том числе в интерактивной форме	50	50
	- лекции (Л)	18	18
	-в том числе в интерактивной форме	18	18
	- практические занятия (ПЗ)	-	-
	-в том числе в интерактивной форме	-	-
	- лабораторные работы (ЛР)	32	32
	-в том числе в интерактивной форме	32	32
2	**Контроль самостоятельной работы (КСР)**	**4**	**4**
3	**Самостоятельная работа студентов (СРС)**	**54**	**54**
	- изучение теоретического материала	18	18
	- расчётно-графические работы	-	-
	- курсовой проект	-	-
	- курсовая работа	-	-
	- реферат	-	-
	- подготовка к аудиторным занятиям (лекциям, лабораторным работам)	18	18
	- подготовка отчетов по лабораторным работам	18	18
	- индивидуальные задания	-	-
	- другие виды самостоятельной работы	-	-
4	Итоговая аттестация по дисциплине: **экзамен**	**36**	**36**
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	Введение	1	1	–	–	–	–	–	**1**
		1	2	2	–	–	–	–	4	**6**
		2	6	2	–	4	–	–	7	**13**
		3	8	2	–	6	–	–	7	**15**
		4	8	2	–	6	–	–	6	**14**
		5	1	1	–	–	–	–	4	**5**
	Итого по модулю:		**26**	**10**	–	**16**	**2**	–	**28**	**56 / 1,6**
2	2	6	6	2	–	4	–	–	7	**13**
		7	8	2	–	6	–	–	7	**15**
		8	8	2	–	6	–	–	7	**15**
		9	1	1	–	–	–	–	5	**6**
		Заключение	1	1	–	–	–	–	–	**1**
	Итого по модулю:		**24**	**8**	–	**16**	**2**	–	**26**	**52 / 1,4**
Итоговая аттестация			–	–	–	–	–	экзамен	–	**36**
Всего:			**50**	**18**	**-**	**32**	**4**	**36**	**54**	**144/4**

4.2 Содержание разделов и тем учебной дисциплины

Модуль 1. Раздел 1. Понятие информационной безопасности. Источники опасности для информации.

Л – 10 ч, ЛР - 16 ч, СРС – 28 ч.

Введение.

Основные определения и понятия. Основы информационной безопасности и защиты информации.

Тема 1. Основные определения и понятия. Основы информационной безопасности и защиты информации.

Основные понятия и определения: информация. Система обработки информации. Объект информатизации. Информационные ресурсы (активы). Защищаемая информация. Безопасность информации. Защита информации. Парольная система. Техническая защита информации. Физическая защита информации. Способ защиты информации. Средство защиты информации.

Тема 2. Источники, риски, формы атак на информацию.

Обзор и параметры классификации угроз безопасности информации. Понятие и подходы к построению модели угроз. Основные понятия: угроза, уязвимость, источник угрозы безопасности информации, защита информации от несанкционированного доступа. Классификация угроз информационной безопасности. Угрозы коммерческой информации. Классификация

злоумышленников. Основные методы реализации угроз информационной безопасности. Причины. Виды и каналы утечки информации.

Тема 3. Политика безопасности. Стандарты безопасности.

Политика ИБ: общее понятие и место в системе защиты информации. Организационные вопросы обеспечения безопасности. Современные международные подходы в области управления безопасностью корпоративных информационных систем. Общие критерии безопасности. Действующие стандарты и рекомендации в области информационной безопасности. Регламентирующие документы в области информационной безопасности. Особенности информационной безопасности компьютерных сетей.

Тема 4. Администрирование компьютерных сетей.

Планирование развития сети. Устранение неисправностей сети. Установка и настройка программного обеспечения. Модернизация компьютерного оборудования. Мероприятия по обеспечению безопасности сети. Техническая поддержка пользователей сети.

Тема 5. Организация защиты информационных систем и сетей.

Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом. Алгоритмы аутентификации пользователей. Парольные системы аутентификации: идентификатор пользователя, пароль пользователя, учетная запись пользователя.

Модуль 2. Раздел 2. Средства защиты информации. Криптографическая защита информации.

Л – 8 ч, ЛР - 16 ч, СРС – 26 ч.

Тема 6. Криптопрограммирование.

Криптопрограммирование посредством использования инкрементальных алгоритмов. Основные элементы инкрементальной криптографии. Методы защиты данных посредством инкрементальных алгоритмов маркирования. Вопросы стойкости инкрементальных схем. Применение инкрементальных алгоритмов для защиты от вирусов.

Тема 7. Методы обеспечения надежности программ, используемые для контроля их технологической безопасности.

Исходные данные, определения и условия. Краткий анализ существующих моделей надежности программного обеспечения. Описание модели Нельсона. Оценка технологической безопасности программ на базе метода Нельсона.

Тема 8. Самотестирующиеся и самокорректирующиеся программы.

Вводные замечания. Общие принципы создания двухмодульных вычислительных процедур и методология самотестирования. Устойчивость, линейная и единичная состоятельность. Метод создания самокорректирующейся процедуры вычисления теоретико-числовой функции дискретного экспоненцирования. Метод создания самотестирующейся расчетной программы с эффективным тестирующим модулем. Исследования процесса верификации расчетных программ. Области применения самотестирующихся и самокорректирующихся программ и их сочетаний.

Тема 9. Правовая и организационная поддержка процессов разработки и применения программного обеспечения.

Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Сертификационные испытания программных средств. Безопасность программного обеспечения и человеческий фактор.

Заключение.

Перспективы развития средств защиты программного обеспечения.

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 темы лабораторной работы
1	2	3
1	Тема 2	Анализ программных средств защиты от несанкционированного доступа.
2	Тема 3	Анализ средств безопасности ОС Windows.
3	Тема 4	Анализ уязвимостей данных в ОС Windows.
4	Тема 6	Анализ средств безопасности ASP.NET. Аутентификация.
5	Тема 7	Анализ средств защиты баз данных.
6	Тема 8	Шифрование информации с использованием стандартов DES и RSA.

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	3 1
Тема 2	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	3 1 3
Тема 3	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	2 2 3
Тема 4	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	2 2 2
Тема 5	Подготовка к аудиторным занятиям	4
Тема 6	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	3 1 3

Тема 7	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	3 1 3
Тема 8	Изучение теоретического материала Подготовка к аудиторным занятиям Подготовка отчетов по лабораторным работам	2 1 4
Тема 9	Подготовка к аудиторным занятиям	5
	Итого: в **ч** / в **ЗЕ**	**54/1,5**

4.5.1. Изучение теоретического материала

Студентами на основе современной литературы самостоятельно рассматриваются следующие вопросы:

Тема 1. Конкурсы по выбору стандартов шифрования.

Тема 2. Стандарт шифрования США.

Тема 3. Европейские криптографические схемы.

Тема 4. Стандарт ISO/IEC 18033.

Тема 6. Стандарт шифрования Японии.

Тема 7. Практические рекомендации известных специалистов.

Тема 8. Патенты на алгоритмы и протоколы.

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 предусмотрено.

5 Образовательные технологии, используемые для формирования компетенций

Преподавание дисциплины ведется с применением:

• **Информационных образовательных технологии**: использование электронных образовательных ресурсов, размещенных на кафедральном сайте (itas.pstu.ru) в виде учебно-методических пособий ко всем формам занятий, электронного конспекта лекций, презентаций, учебников для самостоятельного изучении теоретического материала.

• **Междисциплинарного обучения** – использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи.

• **Проблемного обучения** – использование проблемных профессиональных ситуаций на лабораторных занятиях.

• **Опережающего обучения**, как в рамках междисциплинарного, так и дисциплинарного обучения (самостоятельного изучения студентами нового материала до его изучения в ходе аудиторных занятий).

Проведение **лекционных занятий** по дисциплине основывается на активном методе обучения, при которой учащиеся являются активными участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов к лекции, стимулирующих дополнительную к лекциям самостоятельную работу студентов, установление связей с ранее освоенным материалом, а также ассоциативное и логическое мышление.

Проведение **лабораторных занятий** основывается на интерактивном методе обучения. На первых занятиях (модуль 1) используется управляемая преподавателем работа в команде (2 студента за одним компьютером). В рамках завершения изучения (модуля 2) - игровая технология: проведение тренинга - конкурса с участниками-командами или отдельными студентами по отработке элементов практической деятельности. Задания для соперников и исходные дидактические материалы (компоненты и комплектующие изделия ЭВМ, списки программ, тексты или исполняемые файлы программ, таблиц, чертежей и рисунков схем, алгоритмов и т.д.) готовят сами студенты под руководством преподавателя.

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль освоения дисциплинарных частей компетенций проводится в форме контрольной работы для анализа усвоения материала предыдущей лекции.

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);
- контрольные работы (модули 1, 2).

6.3 Итоговый контроль освоения заданных дисциплинарных частей компетенций

1) **Зачёт**

Не предусмотрен.

2) **Экзамен**

Экзамен проводится в аудитории и во время, указанное в расписании проведения экзаменов. К экзамену допускаются студенты, имеющие разрешение деканата и допуск по предмету. Длительность подготовки студента составляет не менее одного академического часа.

Во время экзамена студент может пользоваться рабочей учебной программой по дисциплине. Контроль знаний осуществляется в устной форме по билетам, утвержденным на заседании кафедры и подписанным заведующим кафедрой.

Оценивается каждый ответ на вопрос билета и каждый при необходимости дополнительный вопрос. Итоговая оценка за экзамен по пятибалльной системе объявляется сразу по окончанию собеседования каждому студенту и выставляется в экзаменационную ведомость с указанием номера зачетной книжки и зачетную книжку.

Студенту, использовавшему на экзамене неразрешенные материалы, выставляется неудовлетворительная оценка.

Фонды оценочных средств, включающие типовые задания к лабораторным работам, вопросы к контрольным работам, список вопросов для проведения экзамена, типовые задания, входящие в состав билетов к экзамену, 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**	**Экзамен**
В результате освоения компетенции студент знает:				
– основные понятия и направления в защите программного обеспечения;	+	+	-	+
– источники, риски, формы атак на информацию;	+	+	-	+
– основные стандарты оценивания защищенности;	+	+	-	+
– средства и методы предотвращения вторжений;	+	+	-	+
– основные уязвимости программного обеспечения.	+	+	-	+
В результате освоения компетенции студент умеет:				
– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;	-	-	+	+
– использовать парольные системы аутентификации;	-	-	+	+
– инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;	-	-	+	+
– анализировать регламентирующие документы в области информационной безопасности;	-	-	+	+
– устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.	-	-	+	+
В результате освоения компетенции студент владеет:				

– навыками анализа информационной безопасности;	-	-	+	+
– навыками администрирования безопасности программного обеспечения;	-	-	+	+
– навыками шифрования информации;	-	-	+	+
– навыками обеспечения безопасности данных в ОС Windows;	-	-	+	+
– навыками выявления и устранения уязвимостей программного обеспечения.	-	-	+	+

ТК – текущая контрольная работа по теме;
ПК – промежуточная контрольная работа по модулю;
ЛР – выполнение лабораторных работ с подготовкой отчёта.

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Вид работы	**Распределение по учебным неделям**																		**Итого**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**Р1**									**Р2**									
Лекции	2	2	2	2	2	2	2	2	2	–	–	–	–	–	–	–	–	–	**18**
Лабораторные работы	–	–	–	–	–	–	–	–	–	4	4	4	4	4	4	4	4	–	**32**
КСР	–	–	–	–	–	–	–	–	2	–	–	–	–	–	–	–	–	2	**4**
Изучение теоретического материала	2	2	2	2	2	2	2	2	2	–	–	–	–	–	–	–	–	–	**18**
Подготовка к аудиторным занятиям	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**18**
Подготовка отчетов по лабораторным работам	–	–	–	–	–	–	–	–	–	2	2	2	2	2	2	2	2	2	**18**
Модуль:	**М1**									**М2**									
Дисциплин. контроль																			**экза-мен**

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б3.Б.7 Защита информации	Профессиональный цикл
(индекс и полное название дисциплины)	(цикл дисциплины)

[*] базовая часть цикла
[ ] вариативная часть цикла
[*] обязательная
[ ] 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 [*] бакалавр [ ] магистр	Форма обучения: [*] очная [ ] заочная [ ] очно-заочная
(аббревиатуры направления и профиля)		

2011
(год утверждения учебного плана ООП)

Семестр(-*ы*): 7

Количество групп: 2

Количество студентов: 30

Мехоношин А.С., ассистент
Электротехнический факультет
Кафедра информационных технологий автоматизированных систем
Тел: (342) 239 13 54

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	Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Государственный университет управления .— М. : Проспект, 2008, 2010.— 333 с.	10
2	Защита информации : учебник для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; Под ред. В. П. Мельникова .— Москва : Академия, 2014 .— 296 с.	6
	2 Дополнительная литература	
	2.1 Учебные и научные издания	
1	Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин ; Под ред. В.Ф. Шаньгина .— 2-е изд., перераб. и доп	11

	.— М. : Радио и связь, 2001 .— 376 с.	
2	Информационная безопасность : учебное пособие для вузов / В.А. Семененко ; Московский государственный индустриальный университет .— 2-е изд., стер .— М. : Изд-во МГИУ, 2006 .— 276 с.	10
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 14.09.2015

Основная литература [*] обеспечена [ ] не обеспечена

Дополнительная литература [*] 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

Таблица 8.2 – Используемые аудио- и видео-пособия

Вид аудио-, видео-пособия				Наименование учебного пособия
теле-фильм	кино-фильм	слайды	аудио-пособие	
1	2	3	4	5
		+		*Презентации к электронному конспекту лекций по дисциплине*

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*	*126 к.А.*	*36*	*19*

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*	*13*	*Оперативное управление*	*126 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

«Защита информации»

(*наименование дисциплины по учебному плану*)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа академическогобакалавриата

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: 4 . **Семестр**: 7

Трудоёмкость:

Кредитов по рабочему учебному плану: 4 ЗЕ

Часов по рабочему учебному плану: 144 ч

Виды контроля:

Экзамен: **-7 сем.** Зачёт: **-нет** Курсовой проект: **-нет** Курсовая работа: **- нет**

Пермь 2016

Учебно-методический комплекс дисциплины «Защита информации» 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», «Математика (Алгебра и геометрия, Математический анализ)», «Информатика 1», «Дискретная математика и теория автоматов», «Введение в профессию», «Моделирование систем», «Системный анализ и управление», «Основы предпринимательской деятельности», «Инновации в информационных технологиях», «Теория дискретных систем», «Разработка средств защиты программного обеспечения», «Методы параллельного программирования», участвующих в формировании компетенций совместно с данной дисциплиной.

1 Общие положения

1.1 Цель учебной дисциплины

Целью изучения дисциплины является получение знаний в области теоретических основ защиты информации и практических навыков обеспечения защиты программного обеспечения.

В процессе изучения данной дисциплины студент осваивает следующие компетенции:

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

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-5).

1.2 Задачи учебной дисциплины

– ***Изучение*** основных методов и средств защиты информации.

– ***Формирование умений*** в области технологии защиты программного обеспечения.

– ***Формирование навыков***, необходимых для разработки средств защиты программного обеспечения.

1.3 Предметом освоения дисциплины являются следующие объекты:

– основные типы угроз;
– основные способы защиты от угроз;
– технические средства защиты;
– организационные и юридические средства защиты;
– основы разработки средств защиты.

1.4 Место учебной дисциплины в структуре образовательной программы.

Дисциплина относится к вариативной части Блока 1. Дисциплины (модули) и является обязательной 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:

– основные понятия и направления в защите программного обеспечения;
– источники, риски, формы атак на информацию;
– основные стандарты оценивания защищенности;
– средства и методы предотвращения вторжений;
– основные уязвимости программного обеспечения.

уметь:

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;
– использовать парольные системы аутентификации;
– инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;
– анализировать регламентирующие документы в области информационной безопасности;
– устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.

владеть:

– навыками анализа информационной безопасности;

- навыками администрирования безопасности программного обеспечения;
- навыками шифрования информации;
- навыками обеспечения безопасности данных в ОС Windows;
- навыками выявления и устранения уязвимостей программного обеспечения.

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», «Основы предпринимательской деятельности», «Разработка средств защиты программного обеспечения»	-
Общепрофессиональные компетенции			
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	«Математика (Алгебра и геометрия, Математический анализ)», «Информатика 1», «Дискретная математика и теория автоматов», «Введение в профессию», «Моделирование систем», «Системный анализ и управление», «Инновации в информационных технологиях», «Теория дискретных систем»	-

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

Учебная дисциплина обеспечивает формирование частей компетенций ОК-4, ОПК-5.

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.В.02	способность использовать основы правовых знаний в области защиты информации в профессиональной деятельности

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – основные понятия и направления в защите программного обеспечения; – источники, риски, формы атак на информацию.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Вопросы к контрольным работам. Вопросы к экзамену.
В результате освоения компетенции студент умеет: – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты; – использовать парольные системы аутентификации.	Лабораторные работы. Самостоятельная работа студентов.	Типовые задания к лабораторным работам. Задания к экзамену.

В результате освоения компетенции студент владеет: – навыками анализа информационной безопасности; – навыками администрирования безопасности программного обеспечения.	Лабораторные работы. Самостоятельная работа студентов.	Типовые задания к лабораторным работам. Задания к экзамену.

2.2 Дисциплинарная карта компетенции ОПК-5

Код	Формулировка компетенции
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Код	Формулировка дисциплинарной части компетенции
ОПК-5.Б1.В.02	способность решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции студент знает: – основные стандарты оценивания защищенности; – средства и методы предотвращения вторжений; – основные уязвимости программного обеспечения.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Вопросы к контрольным работам. Вопросы к экзамену.
В результате освоения компетенции студент умеет: – инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; – анализировать регламентирующие документы в области информационной безопасности; – устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.	Лабораторные работы. Самостоятельная работа студентов.	Типовые задания к лабораторным работам. Задания к экзамену.
В результате освоения компетенции студент владеет: – навыками шифрования информации; – навыками обеспечения безопасности данных в ОС Windows; – навыками выявления и устранения уязвимостей программного обеспечения.	Лабораторные работы. Самостоятельная работа студентов.	Типовые задания к лабораторным работам. Задания к экзамену.

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 изложить в редакции, приведенной на стр. 1а, 2а, 3а, 4а, 5а 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
	Раздел 3 «Структура учебной дисциплины по видам и формам учебной работы» дополнить новым абзацем следующего содержания: «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».	
	В табл. 3.1.: а) строку п.1 «Аудиторная работа» дополнить словами «(контактная работа)»; б) строку п.4 «Итоговая аттестация по дисциплине: экзамен» изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине: экзамен».	
	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.Б.7» на «Б1.В.02»; - 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».	