

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



**Пермский национальный исследовательский  
политехнический университет**

**УТВЕРЖДАЮ**

Проректор по образовательной  
деятельности

 А.Б. Петроченков

« 15 » мая 20 23 г.

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Дисциплина:** Информационная безопасность и защита информации  
(наименование)

**Форма обучения:** очная  
(очная/очно-заочная/заочная)

**Уровень высшего образования:** бакалавриат  
(бакалавриат/специалитет/магистратура)

**Общая трудоёмкость:** 144 (4)  
(часы (ЗЕ))

**Направление подготовки:** 09.03.02 Информационные системы и технологии  
(код и наименование направления)

**Направленность:** Информационные системы и технологии (общий профиль,  
СУОС)  
(наименование образовательной программы)

## 1. Общие положения

### 1.1. Цели и задачи дисциплины

Целями освоения дисциплины являются формирование комплекса знаний основных типов и способов защиты информации, а также умений и навыков применять полученные знания в профессиональной деятельности.

В результате изучения дисциплины обучающийся должен быть способен обеспечить защиту информации в рамках практического решения задач с использованием современных технических средств и программного обеспечения.

### 1.2. Изучаемые объекты дисциплины

- теоретические основы информационной безопасности и защиты информации;
- правовые основы информационной безопасности и защиты информации;
- аппаратные средства обеспечения информационной безопасности;
- программные средства обеспечения информационной безопасности.

### 1.3. Входные требования

Предшествующие дисциплины:

- Информатика;
- Инфокоммуникационные системы и сети
- Теория информации.

## 2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-3	ИД-1ОПК-3	Знает основы теории информации (понятие информации, её свойства); основные разделы информационной безопасности и защиты информации; основные нормативные правовые акты в области информационной безопасности и защиты информации.	Знает возможности и ограничения современных информационно-коммуникационных технологий; основные принципы и нормативные правовые акты информационной безопасности и защиты информации	Дифференцированный зачет

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-3	ИД-2ОПК-3	Умеет использовать полученные знания при решении задач информационной безопасности и защиты информации с использованием современных технических средств и программного обеспечения; пользоваться нормативными документами по защите информации.	Умеет выбирать информационно-коммуникационные технологии, необходимые для эффективного решения стандартных задач в области профессиональной деятельности с учетом требований информационной безопасности	Дифференцированный зачет
ОПК-3	ИД-3ОПК-3	Владеет навыками использования методов информационной безопасности и защиты информации в рамках практического решения задач с применением современных технических средств и программного обеспечения; владеет навыками работы с нормативными правовыми актами	Владеет информационной и библиографической культурой, навыками обеспечения информационной безопасности и защиты информации при решении стандартных задач в области профессиональной деятельности	Кейс-задача
ОПК-5	ИД-1ОПК-5	Знает основные требования к программному обеспечению для защиты информации.	Знает требования к программному обеспечению для информационных систем	Дифференцированный зачет
ОПК-5	ИД-2ОПК-5	Умеет выбирать программное обеспечение для реализации необходимого уровня информационной безопасности.	Умеет выбирать программное обеспечение для повышения эффективности информационных систем	Дифференцированный зачет
ОПК-5	ИД-3ОПК-5	Владеет навыками инсталляции и настройки программного обеспечения, реализующего необходимый уровень информационной безопасности.	Владеет навыками инсталляции программного обеспечения для информационных систем	Кейс-задача

### 3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		6	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	54	54	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	18	18	
- лабораторные работы (ЛР)			
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	32	32	
- контроль самостоятельной работы (КСР)	4	4	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	90	90	
2. Промежуточная аттестация			
Экзамен			
Дифференцированный зачет	9	9	
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	144	144	

### 4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
<b>6-й семестр</b>				
Основы информационной безопасности и защиты информации	6	0	10	20
Тема 1. Понятие национальной безопасности. Угрозы информационной безопасности (ИБ). Модели, стратегии и системы обеспечения ИБ Тема 2. Правовое обеспечение информационной безопасности. Тема 3. Организационное обеспечение ИБ.				
Методы и средства информационной безопасности и защиты информации	6	0	12	30
Тема 4. Технические средства реализации защиты в информационных системах. Тема 5. Общесистемные основы защиты информации и процесса ее обработки. Тема 6. Защита от несанкционированного доступа к компьютерным ресурсам и защита программных средств. Тема 7. Защита от компьютерных вирусов. Тема 8. Математические и методические средства защиты.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Практические вопросы информационной безопасности и защиты информации	6	0	10	40
Тема 9. Уничтожение остаточных данных. Тема 10. Защита от потери информации и отказов программно-аппаратных средств. Тема 11. Защита информационно-программного обеспечения на уровне операционных систем (ОС). Тема 12. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях. Тема 13. Защита информации на уровне систем управления базами данных.				
ИТОГО по 6-му семестру	18	0	32	90
ИТОГО по дисциплине	18	0	32	90

#### Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Анализ надежности пароля
2	Разработка частной модели угроз информационной безопасности
3	Разработка программы разграничения полномочий пользователей на основе парольной аутентификации
4	Криптографическая защита информации
5	Анализ устойчивости парольной защиты
6	Частотный криптоанализ

#### Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Разработка программных средств компьютерной стеганографии: «Соккрытие и извлечение информации в текстовых файлах»
2	Аутентификация пользователей по клавиатурному почерку
3	Криптоанализ шифра Виженера
4	Анализ устойчивости криптостойких хеш функций методу прямого перебора

## 5. Организационно-педагогические условия

### 5.1. Образовательные технологии, используемые для формирования компетенций

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, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и принятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

### 5.2. Методические указания для обучающихся по изучению дисциплины

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 практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.
4. 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.

## 6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

### 6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
<b>1. Основная литература</b>		
1	Данилов А. Н., Лобков А. Л. Инженерно-техническая защита информации : учебное пособие. Пермь : Изд-во ПГТУ, 2007. 339 с.	68
2	Информационная безопасность и защита информации : учебное пособие для вузов / Громов Ю. Ю., Драчев В. О., Иванова О. Г., Шахов Н. Г. Старый Оскол : ТНТ, 2010. 383 с.	5
3	Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации : учебное пособие для вузов. 3-е изд., стер. Москва : Академия, 2008. 331 с.	25
<b>2. Дополнительная литература</b>		
<b>2.1. Учебные и научные издания</b>		
1	Данилов А. Н., Лобков А. Л. Инженерно-техническая защита информации : учебное пособие. Пермь : Изд-во ПГТУ, 2007. 339 с.	68

2	Данилов А.Н., Шабуров А.С. Организационное обеспечение информационной безопасности : учебное пособие. Пермь : Изд-во ПГТУ, 2007. 257 с	80
<b>2.2. Периодические издания</b>		
1	Журнал «Информационные технологии»	
<b>2.3. Нормативно-технические издания</b>		
	Не используется	
<b>3. Методические указания для студентов по освоению дисциплины</b>		
	Не используется	
<b>4. Учебно-методическое обеспечение самостоятельной работы студента</b>		
	Не используется	

## 6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Информационная безопасность : учебное пособие / Лои?ко В. И., Лаптев В. Н., Аршинов Г. А., Лаптев С. Н. Краснодар : КубГАУ, 2020. 332 с.	<a href="https://elib.pstu.ru/Record/lanRU-LAN-BOOK-254168">https://elib.pstu.ru/Record/lanRU-LAN-BOOK-254168</a>	сеть Интернет; авторизованный доступ

## 6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567

## 6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных научной электронной библиотеки (eLIBRARY.RU)	<a href="https://elibrary.ru/">https://elibrary.ru/</a>
Научная библиотека Пермского национального исследовательского политехнического университета	<a href="http://lib.pstu.ru/">http://lib.pstu.ru/</a>
Электронно-библиотечная система Лань	<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>
Электронно-библиотечная система IPRbooks	<a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>
Информационные ресурсы Сети КонсультантПлюс	<a href="http://www.consultant.ru/">http://www.consultant.ru/</a>

## **7. Материально-техническое обеспечение образовательного процесса по дисциплине**

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Мультимедиа-проектор	1
Курсовая работа	Ноутбук	1
Лекция	Мультимедиа-проектор	1
Лекция	Ноутбук	1
Практическое занятие	Мультимедиа-проектор	1
Практическое занятие	Ноутбук	1

## **8. Фонд оценочных средств дисциплины**

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение  
высшего образования

**Пермский национальный исследовательский  
политехнический университет**

Факультет прикладной математики и механики  
Кафедра «Вычислительная математика, механика и биомеханика»

### **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**для проведения промежуточной аттестации обучающихся по дисциплине  
«Информационная безопасность и защита информации»**

#### *Приложение к рабочей программе дисциплины*

<b>Направление подготовки:</b>	09.03.02 Информационные системы и технологии
<b>Профиль программы бакалавриата:</b>	Цифровые технологии и интеллектуальные системы управления
<b>Квалификация выпускника:</b>	Бакалавр
<b>Выпускающая кафедра:</b>	Вычислительная математика, механика и биомеханика
<b>Форма обучения:</b>	Очная
<b>Форма промежуточной аттестации:</b>	Диф. зачет

**Оценочные материалы** (фонд оценочных средств, ФОС) для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины (РПД). ФОС устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

### 1. Перечень контролируемых результатов обучения по дисциплине

Согласно РПД освоение учебного материала дисциплины запланировано в течение 6-го семестра. В рамках освоения учебного материала дисциплины формируются компоненты компетенций знать, уметь, владеть, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала и промежуточной аттестации. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля						
	Текущий			Промежуточный/ рубежный		Итоговый	
	С	ТО	ПЗ	ОЛР	Т/КР/ КИЗ	К/р	Диф. зачет
<b>Усвоенные знания</b>							
<b>З.1</b> знать основы теории информации (понятие информации, её свойства); основные разделы информационной безопасности и защиты информации; основные нормативные правовые акты в области информационной безопасности и защиты информации	С	ТО			КР		ТВ
<b>З.2</b> знать основные требования к программному обеспечению для защиты информации	С	ТО			КР		ТВ
<b>Освоенные умения</b>							
<b>У.1</b> уметь использовать полученные знания при решении задач информационной безопасности и защиты информации с использованием современных технических средств и программного обеспечения; пользоваться нормативными документами по защите информации					КР		ПЗ
<b>У.2</b> уметь выбирать программное обеспечение для реализации необходимого уровня информационной безопасности					КР		ПЗ
<b>Приобретенные владения</b>							
<b>В.1</b> владеть навыками использования методов информационной безопасности и защиты информации в рамках практического решения задач с применением современных технических средств и программного обеспечения; владеет навыками работы с нормативными правовыми актами						КИЗ	ПЗ
<b>В.2</b> владеть навыками инсталляции и настройки программного обеспечения, реализующего необходимый уровень информационной безопасности						КИЗ	ПЗ

*С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КИЗ – кейс-задача (комплексное индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР –*

*рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.*

Итоговой оценкой освоения дисциплинарных частей компетенций (результатов обучения по дисциплине) является промежуточная аттестация в виде диф. зачета, проводимая с учетом результатов текущего и рубежного контроля.

## **2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения**

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

### **2.1. Текущий контроль усвоения материала**

Текущий контроль усвоения материала в форме собеседования, выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

### **2.2. Промежуточный и рубежный контроль**

Промежуточный и рубежный контроль для комплексного оценивания усвоенных знаний, усвоенных умений (табл. 1.1) проводится в форме защиты лабораторных (практических) работ и рубежных контрольных работ.

### **2.2.1. Защита лабораторных работ**

Лабораторных работ по дисциплине не предусмотрено.

### **2.2.2. Рубежная контрольная работа**

Согласно РПД запланированы рубежные контрольные работы по разделам дисциплины.

#### **Типовые задания КР:**

1. Понятие информационной безопасности.
2. Классификация угроз информационной безопасности.
3. Описать требования для выбора надежного пароля. Дать количественную оценку устойчивости предложенных паролей.

Типовые шкала и критерии оценки результатов рубежной контрольной работы приведены в общей части ФОС программы бакалавриата.

### **2.2.3. Выполнение комплексного индивидуального задания на самостоятельную работу**

Комплексных индивидуальных заданий по дисциплине не предусмотрено.

### **2.3. Промежуточная аттестация (итоговый контроль)**

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде диф. зачета по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки усвоенных умений, а также может содержать комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных дисциплинарных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности *всех* заявленных дисциплинарных компетенций. Форма билета представлена в общей части ФОС программы бакалавриата.

#### **2.3.1. Типовые вопросы и задания для диф. зачета по дисциплине**

##### **Типовые вопросы для контроля усвоенных знаний:**

1. Понятие информационной безопасности.
2. Основные нормативно-правовые акты в области защиты информации.
3. Понятие информации и ее свойства.
4. Основные меры обеспечения безотказности информационной системы.

##### **Типовые практические задания для контроля усвоенных умений и приобретенных владений:**

1. Описать требования для выбора надежного пароля. Дать количественную оценку устойчивости предложенных паролей к методу прямого перебора с известной мощностью.

2. Используя метод Виженера произвести шифрование/дешифрование текстового сообщения.

3. Используя метод перестановки произвести шифрование/дешифрование текстового сообщения.

4. Описать организационные меры информационной безопасности, которые

вы используете быту, привести примеры их использования в учебном процессе.

### **2.3.2. Шкалы оценивания результатов обучения при диф. зачете**

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных дисциплинарных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время диф. зачета.

Типовые шкала и критерии оценки результатов обучения при диф. зачете для компонентов *знать, уметь и владеть* приведены в общей части ФОС программы бакалавриата.

### **2.3.3. Защита курсовых работ**

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, выполняется курсовая работа с использованием комплексных индивидуальных заданий.

Типовые темы курсовых работ приведены в РПД.

Защита курсовых работы проводится индивидуально каждым студентом или группой студентов. Типовые шкала и критерии оценки курсовых работ приведены в общей части ФОС образовательной программы.

## **3. Критерии оценивания уровня сформированности компонентов и дисциплинарных компетенций**

### **3.1. Оценка уровня сформированности компонентов дисциплинарных компетенций**

При оценке уровня сформированности дисциплинарных компетенций в рамках выборочного контроля при диф. зачете считается, что полученная оценка за компонент проверяемой в билете дисциплинарной компетенции обобщается на соответствующий компонент всех дисциплинарных компетенций, формируемых в рамках данной учебной дисциплины.

Типовые критерии и шкалы оценивания уровня сформированности компонентов дисциплинарных компетенций приведены в общей части ФОС программы бакалавриата.

### **3.2. Оценка уровня сформированности дисциплинарных компетенций**

Общая оценка уровня сформированности всех дисциплинарных компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС программы бакалавриата.

При формировании итоговой оценки промежуточной аттестации в виде диф. зачета используются типовые критерии, приведенные в общей части ФОС программы бакалавриата.