

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



**Пермский национальный исследовательский  
политехнический университет**

**УТВЕРЖДАЮ**

Проректор по учебной работе

  
\_\_\_\_\_ Н.В.Лобов

« 22 » января 20\_\_ г.

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Дисциплина:** Инженерия вредоносного и защитного программного обеспечения

\_\_\_\_\_  
(наименование)

**Форма обучения:** \_\_\_\_\_ очная

(очная/очно-заочная/заочная)

**Уровень высшего образования:** \_\_\_\_\_ магистратура

(бакалавриат/специалитет/магистратура)

**Общая трудоёмкость:** \_\_\_\_\_ 216 (6)

(часы (ЗЕ))

**Направление подготовки:** \_\_\_\_\_ 09.04.04 Программная инженерия

(код и наименование направления)

**Направленность:** \_\_\_\_\_ Разработка программно-информационных систем

(наименование образовательной программы)

## 1. Общие положения

### 1.1. Цели и задачи дисциплины

Цель учебной дисциплины – изучение современных средств и методов защиты компьютерной информации от несанкционированного доступа: средств современных операционных систем, криптографических алгоритмов, межсетевых экранов, научиться применять стандартные прикладные пакеты для обеспечения безопасности информации, а также проектировать собственные средства защиты.

Задачи учебной дисциплины:

- изучение средств защиты, стандартов оценки защищенности и основных уязвимостей программного обеспечения.
- формирование умения осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств.
- формирование навыков администрирования безопасности, выявления и устранения уязвимостей программного обеспечения.

### 1.2. Изучаемые объекты дисциплины

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.

### 1.3. Входные требования

Не предусмотрены

## 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
ПК-2.1	ИД-1ПК-2.1	Знает политику и стандарты безопасности; методы обеспечения надежности программ	Знает методологии разработки программного обеспечения	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.1	ИД-2ПК-2.1	Умеет устанавливать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты	Умеет применять нормативные документы, определяющие требования к оформлению программного кода	Экзамен
ПК-2.1	ИД-3ПК-2.1	Владеет навыками администрирования безопасности программного обеспечения; навыками выявления и устранения уязвимостей программного обеспечения.	Владеет навыками оценки качества и эффективности программного кода	Защита лабораторной работы
ПК-2.3	ИД-1ПК-2.3	Знает: основные понятия информационной безопасности и защиты информации; источники, риски, формы атак на информацию; политику и стандарты безопасности; методы обеспечения надежности программ; правовую и организационную поддержку процессов разработки и применения программного обеспечения.	Знает нормативно-технические документы (стандарты и регламенты), лучшие мировые практики и внутренние нормативные документы в части разработай требований к программному обеспечению;	Экзамен
ПК-2.3	ИД-2ПК-2.3	Умеет: устанавливать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;	Умеет применять методы и средства разработки технических спецификаций программного обеспечения;	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.		
ПК-2.3	ИД-ЗПК-2.3	Владеет: навыками анализа информационной безопасности; навыками администрирования безопасности программного обеспечения; навыками выявления и устранения уязвимостей программного обеспечения.	Владеет навыками распределение заданий на разработку технических спецификаций программного обеспечения.	Защита лабораторной работы

### 3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		2	
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)	18	18	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	16	16	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	126	
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	216	216	

### 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

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
2-й семестр				
Вредоносные программы.	10	4	8	62
Тема 1. Введение в теорию обеспечения безопасности программ и данных. Введение в теорию обеспечения безопасности программ и данных. Понятие о вредоносных программах. Виды компьютерных вирусов. Возможные последствия действий вредоносных программ. Антивирусные программы и их классификация. Тема 2. Оценка надежности защитных механизмов. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка надежности защитных механизмов. Расчет вероятности наличия разрушающих программных средств на этапе испытаний программного обеспечения и подходы к его исследованию. Методы и средства анализа безопасности программ и данных. Методы защиты информации в вычислительных сетях.				
Защита программ и данных.	8	14	8	64
Тема 3. Защита программ Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Защита программ от изучения. Защита программ от несанкционированного использования. Защита программного обеспечения, основанная на идентификации: пользователя; ПЭВМ; исполняемого модуля. Виды ключей для ПО и их проверки. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности. Программно-аппаратные средства защиты ЭВМ. Методы и средства ограничения доступа к компонентам ЭВМ. Методы и средства хранения ключевой информации. Тема 4. Защита данных. Методы криптографии. Защита данных от изменения и контроль целостности. Модель Кларка-Вилсона. Шифрование данных и программ. Понятие идеального шифра. Организация комплексной защиты информационных систем. Организация защиты программного обеспечения.				
ИТОГО по 2-му семестру	18	18	16	126
ИТОГО по дисциплине	18	18	16	126

## Тематика примерных практических занятий

<b>№ п.п.</b>	<b>Наименование темы практического (семинарского) занятия</b>
1	Установка и настройка антивирусной программы.
2	Разработка вирусной программы. Оценка действия антивирусной программы.
3	Защита программ от изучения. Защита программ от несанкционированного использования.
4	Защита программного обеспечения, основанная на идентификации: пользователя; ПЭВМ; исполняемого модуля.
5	Использование отечественного электронного ключа «РуТокен».
6	Использование зарубежного электронного ключа «SenseLock». Изучение работы с электронными замками («Соболь», «Аккорд») и биометрическими защитами («Еyes OptiMouse»).
7	Защита данных от изменения и контроль целостности.
8	Шифрование данных и программ.

## Тематика примерных лабораторных работ

<b>№ п.п.</b>	<b>Наименование темы лабораторной работы</b>
1	Разработка вирусной программы.
2	Разработка антивирусной программы – ревизора диска.
3	Защита программного обеспечения, основанная на идентификации: пользователя; ПЭВМ; исполняемого модуля.
4	Защита программы электронным ключом.
5	Защита данных от изменения и контроль целостности.
6	Шифрование данных и программ.

## 5. Организационно-педагогические условия

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

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой 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 установления 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.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

### 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	Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. - Санкт-Петербург: ВHV-СПб, 2000.	7
2	Хогланд Г. Взлом программного обеспечения: анализ и использование кода : пер. с англ. / Г. Хогланд, Г. Мак-Гроу. - М.: Вильямс, 2005.	7
<b>2. Дополнительная литература</b>		

<b>2.1. Учебные и научные издания</b>		
1	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных : учебное пособие / П. Ю. Белкин [и др.]. - Москва: Радио и связь, 1999.	9
2	Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях / С. П. Расторгуев. - Москва: Яхтсмен, 1993.	4
<b>2.2. Периодические издания</b>		
	Не используется	
<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	Никифоров С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие / Никифоров С. Н. - Санкт-Петербург: Лань, 2019.	<a href="http://elib.pstu.ru/Record/lanRU-LAN-BOOK-114697">http://elib.pstu.ru/Record/lanRU-LAN-BOOK-114697</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	MS Windows 8.1 (подп. Azure Dev Tools for Teaching )
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Среды разработки, тестирования и отладки	Microsoft Visual Studio (подп. Azure Dev Tools for Teaching )

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

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	<a href="http://lib.pstu.ru/">http://lib.pstu.ru/</a>



Наименование	Ссылка на информационный ресурс
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
Лабораторная работа	ПЭВМ	10
Лекция	Компьютер, мультимедийный проектор, экран.	1
Практическое занятие	ПЭВМ	10

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

Описан в отдельном документе
------------------------------