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

« 29 » мая 20 23 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Дисциплина:** Теоретические основы компьютерной безопасности
(наименование)

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

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

**Общая трудоёмкость:** 216 (6)
(часы (ЗЕ))

**Направление подготовки:** 10.04.01 Информационная безопасность
(код и наименование направления)

**Направленность:** Комплексные системы информационной безопасности
(наименование образовательной программы)

Пермь 2023

## 1. Общие положения

### 1.1. Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности компьютерных информационных систем и освоение компетенций для решения основных задач защиты информации в информационных системах
Задачи дисциплины:
- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации;
- приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

### 1.2. Изучаемые объекты дисциплины

- основные понятия, общеметодологические принципы теории информационной безопасности;
- виды средств защиты информации в компьютерных информационных системах;
- угрозы безопасности информации и уязвимости компьютерных информационных систем;
- методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды каналы утечки информации и несанкционированного доступа;
- формальные модели безопасности информации;
- уровни и сервисы защиты информации;
- критерии оценки защищенности информационных систем;
- основы организации защиты информации на предприятии.

### 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-1.1 | ИД-1ПК-1.1 | Знает способы снижения рисков реализации угроз в компьютерных системах с применением аппаратных и программных средств | Знает способы реализации угроз безопасности в автоматизированных системах | Защита лабораторной работы |
| ПК-1.1 | ИД-2ПК-1.1 | Умеет анализировать возможные уязвимости компьютерных систем | Умеет анализировать возможные уязвимости информационных систем | Экзамен |

| Компетенция | Индекс индикатора | Планируемые результаты обучения по дисциплине (знать, уметь, владеть) | Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения | Средства оценки |
|---|---|---|---|---|
| ПК-1.1 | ИД-3ПК-1.1 | Владеет навыками моделирования и обработки полученной информации для составления модели компьютерной системы | Владеет навыками систематизации результатов проведенных исследований | Защита лабораторной работы |
| ПКО-1 | ИД-1ПКО-1 | Знает основные критерии оценки защищённость компьютерной сети | Знает основные требования, необходимые для организации и обес-печения защиты информации в автома-тизированной системе | Экзамен |
| ПКО-1 | ИД-2ПКО-1 | Умеет собирать, изучать и систематизировать информацию, для создания модели компьютерной системы и дальнейшего обеспечения защиты информации в автоматизированной системе, с учётом характера информационных процессов протекающих в ней. | Умеет собирать, изучать и систематизировать информацию, для организации и обеспечения защиты информации в автоматизированной системе | Защита лабораторной работы |
| ПКО-1 | ИД-3ПКО-1 | Владеет навыками составления моделей компьютерной системы с учётом нормативно правовых актов | Владеет навыками сбора и обработки данных в сфере поиска, отбора и анализа информации для обеспечения защиты информации | Деловая игра |

## 3. Объем и виды учебной работы

| Вид учебной работы | Всего часов | Распределение по семестрам в часах |
|---|---|---|
| | | Номер семестра |
| | | 3 |
| 1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:<br>1.1. Контактная аудиторная работа, из них: | 54 | 54 |
| - лекции (Л) | 18 | 18 |
| - лабораторные работы (ЛР) | 32 | 32 |
| - практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ) | | |
| - контроль самостоятельной работы (КСР) | 4 | 4 |
| - 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 |
| 3-й семестр | | | | |
| Моели копьютерных систем | 8 | 16 | 0 | 63 |
| Изучение общепринятых моделей компьютерных систем, изучения способов их применения при моделировании систем безопасности. Изучение основных угроз информационной безопасности в компьютерных системах. | | | | |
| Методы и средства защиты компьютерных систем | 10 | 16 | 0 | 63 |
| Изучение модели нарушителя информационной безопасности. Изучение средств и методов защиты компьютерных систем. | | | | |
| ИТОГО по 3-му семестру | 18 | 32 | 0 | 126 |
| ИТОГО по дисциплине | 18 | 32 | 0 | 126 |

Тематика примерных лабораторных работ

| № п.п. | Наименование темы лабораторной работы |
|---|---|
| 1 | Тунелирование информации и VPN |

| № п.п. | Наименование темы лабораторной работы |
|---|---|
| 2 | Резервирование и архивирование информации |
| 3 | Моделирование оносительной пропускной способности компьютерной системы |

## 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.

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 лабораторным работам.
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 |
|---|---|---|
| **1. Основная литература** | | |
| 1 | Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. - Санкт-Петербург: BHV-СПб, 2000. | 7 |
| 2 | Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие для вузов / В. И. Завгородний. - Москва: Логос, 2001. | 27 |
| **2. Дополнительная литература** | | |
| **2.1. Учебные и научные издания** | | |

| | | |
|---|---|---|
| 1 | Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М.Батурин,А.М.Жодзишский. - М.: Юрид. лит., 1991. | 2 |
| 2 | Запечников С. В. Основы построения виртуальных частных сетей : учебное пособие для вузов / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. - Москва: Горячая линия-Телеком, 2011. | 15 |
| 3 | Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - Москва: ДМК, 2000. | 1 |
| 4 | Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для вузов / А. Ю. Щербаков. - М.: Кн. мир, 2009. | 5 |
| **2.2. Периодические издания** | | |
| | Не используется | |
| **2.3. Нормативно-технические издания** | | |
| | Не используется | |
| **3. Методические указания для студентов по освоению дисциплины** | | |
| 1 | Бабаев С. И. Компьютерные сети. Лабораторный практикум : учебное пособие для вузов / С. И. Бабаев, М. Б. Никифоров. - Москва: КУРС, 2020. | 1 |
| 2 | Дэвис П. Т. Компьютерная безопасность для чайников: [Для сомневающихся] : пер. с англ / П. Т. Дэвис, Б. Д. Льюис. - Киев Москва: Диалектика, 1997. | 1 |
| 3 | Информатика. Базовый курс : учебное пособие для втузов / С. В. Симонович [и др.]. - Санкт-Петербург [и др.]: Питер, 2005. | 27 |
| 4 | Карпов Ю. Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5 / Ю. Г. Карпов. - СПб: БХВ-Петербург, 2006. | 4 |
| 5 | Колесников Олег Linux: создание виртуальных частных сетей (VPN) / ОлегКолесников,БрайанХетч. - М.: КУДИЦ-ОБРАЗ, 2004. | 1 |
| **4. Учебно-методическое обеспечение самостоятельной работы студента** | | |
| | 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 | Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск: Сибирскии? федеральныи? университет, 2019. | http://elib.pstu.ru/Record/iprbooks100055 | 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. | Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF |
| Офисные приложения. | Microsoft Office Professional 2007. лиц. 42661567 |
| Прикладное программное обеспечение общего назначения | Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017 |

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

| Наименование | Ссылка на информационный ресурс |
|---|---|
| Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю | https://bdu.fstec.ru/ |
| Научная библиотека Пермского национального исследовательского политехнического университета | http://lib.pstu.ru/ |
| Электронно-библиотечеая система Лань | https://e.lanbook.com/ |
| Электронно-библиотечная система IPRbooks | http://www.iprbookshop.ru/ |
| Информационные ресурсы Сети КонсультантПлюс | http://www.consultant.ru/ |
| База данных компании EBSCO | https://www.ebsco.com/ |

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

| Вид занятий | Наименование необходимого основного оборудования и технических средств обучения | Количество единиц |
|---|---|---|
| Лабораторная работа | Персональный компьютер | 10 |
| Лекция | Мультимедийный проектор | 1 |
| Лекция | Персональный компьютер | 10 |

## 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»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
**для проведения промежуточной аттестации обучающихся по дисциплине «Теоретические основы компьютерной безопасности»**
***Приложение к рабочей программе дисциплины***

**Направление подготовки:** 10.04.01 Информационная безопасность

**Направленность (профиль) образовательной программы:** Комплексные системы информационной безопасности

**Квалификация выпускника:** Магистр

**Выпускающая кафедра:** Автоматика и телемеханика

**Форма обучения:** Очная

**Курс:** 2 **Семестр**: 3

**Трудоёмкость:**
Кредитов по рабочему учебному плану: 6 ЗЕ
Часов по рабочему учебному плану: 216 ч.

**Форма промежуточной аттестации:**
Экзамен: 3 семестр

Пермь 2021

**Фонд оценочных средств** для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

## 1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (3-го семестра учебного плана). Предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. 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** | | **Рубежный** | | **Итоговый** | |
| | **С** | **ТО** | **ОЛР** | **Т/КР** | | **Экзамен** |
| **Усвоенные знания** | | | | | | |
| **З.1** знать основные требования, необходимые для организации и обес-печения защиты информации в автома-тизированной системе | | ТО | ОЛР | | | ТВ |
| **Освоенные умения** | | | | | | |
| **У.1** уметь собирать, изучать и систематизировать информацию, для организации и обеспечения защиты информации в автоматизированной системе | | | ОЛР | | | ПЗ |
| **Приобретенные владения** | | | | | | |
| **В.1** владеть сбора и обработки данных в сфере поиска, от-бора и анализа информации для обес-печения защиты информации | | | ОЛР | | | |

*С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.*

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, 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 или 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. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 3 лабораторные работы. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

**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 экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

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

**2.3.1. Типовые вопросы и задания для экзамена по дисциплине**

**Типовые вопросы для контроля усвоенных знаний:**

1. Общепринятые модели компьютерных систем.
2. Способы моделировании систем безопасности.
3. Основных угрозы информационной безопасности в компьютерных системах.
4. Модели нарушителя информационной безопасности.
5. Средства и методы защиты компьютерных систем.

**Типовые вопросы и практические задания для контроля освоенных умений:**

1. Туннелирование информации, VPN.
2. Резервирование и архивирование информации.
3. Относительная пропускная способность информационной системы.

**2.3.2. Шкалы оценивания результатов обучения на экзамене**

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

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

## 3. Критерии оценивания уровня сформированности компонентов и компетенций

**3.1. Оценка уровня сформированности компонентов компетенций**

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент*

*проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

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

**3.2. Оценка уровня сформированности компетенций**

Общая оценка уровня сформированности всех 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 образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Примеры вопросов для проверки знаний:

1. Состояние информации, при котором допуск к ней осуществляют лишь субъекты, которые имеют такое право
✓ Конфиденциальность
o Целостность
o Доступность

2. Избежание несанкционированных изменений информации
o Конфиденциальность
✓ Целостность
o Доступность

3. Избежание постоянного или временного сокрытия информации от субъектов, которые имеют права доступа
o Конфиденциальность
o Целостность
✓ Доступность

4. Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов
✓ Антивирус
o Межсетевой экран (брандмауэр)
o Система обнаружения вторжения

5. Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами
o Антивирус
✓ Межсетевой экран (брандмауэр)
o Система обнаружения вторжения

6. Программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет
o Антивирус
o Межсетевой экран (брандмауэр)
✓ Система обнаружения вторжения

7. Технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети
✓ VPN
o RAID
o IDS

8. Технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности
- o VPN
- ✓ RAID
- o IDS

9. Опишите принцип работы VPN (открытый вопрос)

10. Опишите принцип работы RAID 0 (открытый вопрос)

11. Опишите принцип работы RAID 1 (открытый вопрос)