

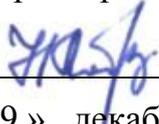
Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования



**Пермский национальный исследовательский  
политехнический университет**

**УТВЕРЖДАЮ**

Проректор по учебной работе

  
\_\_\_\_\_ Н.В.Лобов

« 09 » декабря 20 19 г.

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Дисциплина:** \_\_\_\_\_ Прогнозирование рисков информационной 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)

# 1. Общие положения

## 1.1. Цели и задачи дисциплины

Цель - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности.

Задачи дисциплины:

- изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности;
- изучение предпосылок для управления информационными рисками;
- изучение основных требований по управлению рисками информационной безопасности;
- изучение состава системы управления информационными рисками;
- формирование умений оценки рисков информационной безопасности;
- формирование умений обработки рисков информационной безопасности;
- формирование навыков по оценке угроз безопасности информации в технологии оценки рисков;
- формирование навыков подбора инструментальных средств для управления рисками информационной безопасности.

## 1.2. Изучаемые объекты дисциплины

- современные информационные риски и их особенности;
- стандарты управления рисками;
- стандарты в области управления рисками информационной безопасности;
- система управления информационными рисками;
- порядок оценки рисков информационной безопасности;
- анализ угроз и уязвимостей;
- профиль и жизненный цикл угрозы;
- описание угроз безопасности;
- способы классификации угроз;
- уязвимости информационной безопасности;
- идентификация организационных и технических уязвимостей;
- оценка угроз и уязвимостей;
- определение величины риска;
- процесс и способы обработки рисков;
- инструментальные средства для управления рисками.

## 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 основные риски безопасности информации в автоматизированных системах	Знает способы реализации угроз безопасности в автоматизированных системах	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-1.1	ИД-2ПК-1.1	Умеет анализировать возможные риски, связанные с обработкой информации в информационных системах	Умеет анализировать возможные уязвимости информационных систем	Защита лабораторной работы
ПК-1.1	ИД-3ПК-1.1	Владеет навыками систематизации оценки и обработки рисков информационной безопасности	Владеет навыками систематизации результатов проведенных исследований	Защита лабораторной работы
ПКО-2	ИД-1ПКО-2	Знает подходы к построению и исследованию моделей оценки и обработки рисков информационной безопасности в автоматизированных системах	Знает подходы к построению и исследованию моделей процессов защиты информации в автоматизированных системах	Защита лабораторной работы
ПКО-2	ИД-2ПКО-2	Умеет разрабатывать модели оценки рисков и доказывать адекватность данных моделей для использования в системе защиты информации	Умеет разрабатывать и доказывать адекватность моделей систем защиты информации	Защита лабораторной работы
ПКО-2	ИД-3ПКО-2	Владеет навыками применения программного обеспечения для оценки обработки рисков в задачах моделирования и исследования моделей систем защиты информации	Владеет навыками применения программного обеспечения в задачах моделирования и исследования моделей систем защиты информации	Защита лабораторной работы

### 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:	54	54	
1.1. Контактная аудиторная работа, из них:			
- 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				
Введение в дисциплину	2	0	0	14
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Особенности формирования терминологии научной дисциплины. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература.				
Предпосылки для управления информационными рисками	2	4	0	14
Современные информационные риски и их особенности. Кибертерроризм. Риски промышленных систем. Риски утечки информации. Риски электронных расчетов. Стандарты управления рисками. Государственное регулирование. Оценка рисков как основа корпоративного управления.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Основные требования по управлению рисками информационной безопасности	2	4	0	14
Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Информационная составляющая бизнес - рисков. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Уровни зрелости бизнеса в от-ношении рисков. Анализ факторов риска. Методика оценки рисков приватности, включая персональные данные				
Система управления информационными рисками	2	4	0	14
Преимущества системного подхода к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками. Процессная модель управления рисками. Непрерывная деятельность по управлению рисками. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства. Пересмотр и переоценка риска. Взаимосвязь процессов аудита и управления рисками. Управление документами и записями. Корректирующие и превентив-ные меры. Коммуникация рисков. Аутсорсинг процессов управления рисками. Распреде-ление ответственности за управление рисками. Требования к риск-менеджеру. Требования к эксперту по оценке рисков.				
Оценка рисков информационной безопасности	2	4	0	14
Идентификация активов. Описание бизнес-процессов. Идентификация требований безопасности. Реестр требований безопасности. Требования законодательства и нормативной базы. Контрактные обязательства. Требования бизнеса. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов. Особенности интервьюирования бизнес-пользователей. Определение приоритетов аварийного восстановления.				
Оценка угроз безопасности информации в технологии оценки рисков	2	4	0	14
Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы. Описание угроз безопасности. Способы классификации угроз. Уязвимости информационной безопасности. Идентификация организационных уязвимостей. Идентификация технических уязвимостей. Оценка				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Пример оценки риска. Отчет об оценке рисков.				
Обработка рисков информационной безопасности	2	4	0	14
Процесс обработки рисков. Способы обработки риска. Принятие риска. Уменьшение риска. Передача риска. Избегание риска. Оценка возврата инвестиций в информационную безопасность. Принятие решения по обработке риска. План обработки рисков. Декларация о применимости механизмов контроля. Профили рисков информационной безопасности.				
Инструментальные средства для управления рисками	2	4	0	14
Актуальность программного сопровождения процедуры оценки рисков. Выбор программного обеспечения для оценки рисков. Общие недостатки и ограничения коммерческих программных продуктов. Обзор методов и инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.				
Внедрение системы прогнозирования и управления рисками информационной безопасности	2	4	0	14
Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками. Обучение членов экспертной группы. Проведение полной оценки рисков по всем активам. Жизненный цикл управления рисками.				
<b>ИТОГО по 3-му семестру</b>	<b>18</b>	<b>32</b>	<b>0</b>	<b>126</b>
<b>ИТОГО по дисциплине</b>	<b>18</b>	<b>32</b>	<b>0</b>	<b>126</b>

### Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Анализ требований и стандартов в области управления рисками информационной безопасности.
2	Исследование современных информационных рисков и их особенностей.
3	Исследование рисков различных информационных систем.
4	Количественное и качественное определение величины риска.
5	Разработка системы управления информационными рисками.
6	Оценка угроз безопасности информации в технологии оценки рисков.

<b>№ п.п.</b>	<b>Наименование темы лабораторной работы</b>
7	Применение технологий обработки рисков информационной безопасности.
8	Методы и инструментальные средства управления рисками.

## 5. Организационно-педагогические условия

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

<p>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.</p> <p>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.</p> <p>При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.</p>
---

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

<p>При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> <li>1. Изучение учебной дисциплины должно вестись систематически.</li> <li>2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.</li> <li>3. Особое внимание следует уделить выполнению отчетов по лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.</li> <li>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.</li> </ol>
--

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

### 6.1. Печатная учебно-методическая литература

<b>№ п/п</b>	<b>Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)</b>	<b>Количество экземпляров в библиотеке</b>
<b>1. Основная литература</b>		
1	Егоров А. Ф. Анализ риска, оценка последствий аварий и управление безопасностью химических, нефтеперерабатывающих и нефтехимических производств : учебное пособие для вузов / А. Ф. Егоров, Т. В. Савицкая. - Москва: КолосС, 2010.	8

2	Милославская Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва: Горячая линия-Телеком, 2014.	15
<b>2. Дополнительная литература</b>		
<b>2.1. Учебные и научные издания</b>		
1	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2	Шапкин А. С. Теория риска и моделирование рискованных ситуаций : учебник для вузов / А. С. Шапкин, В. А. Шапкин. - М.: Дашков и К, 2007.	10
<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	В. А. Горев Надежность технических систем и техногенный риск : Учебно-методическое пособие к практическим работам для обучающихся по направлению подготовки / В. А. Горев. - Москва: МИСИ-МГСУ, Ай Пи Эр Медиа, ЭБС АСВ, 2018	<a href="http://elib.pstu.ru/Record/iprbooks88475">http://elib.pstu.ru/Record/iprbooks88475</a>	сеть Интернет; свободный 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

#### **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>
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>
База данных компании EBSCO	<a href="https://www.ebsco.com/">https://www.ebsco.com/</a>
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	<a href="https://техэксперт.сайт/">https://техэксперт.сайт/</a>

#### **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

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

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