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
« 28 » ноября 20 19 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Безопасность и защита информации в распределенных автоматизированных системах
(наименование)

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

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

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

Направление подготовки: 09.04.04 Программная инженерия
(код и наименование направления)

Направленность: Разработка программно-информационных систем
(наименование образовательной программы)

Пермь 2019

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
ОПК-2	ИД-1ОПК-2	Знает: основные понятия информационной безопасности и защиты информации; источники, риски, формы атак на информацию; методы обеспечения надежности программ.	Знает порядок поиска и систематизации информации об опыте решения научно-технической задачи в сфере профессиональной деятельности	Дифференцированный зачет
ОПК-2	ИД-2ОПК-2	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты.	Умеет формулировать научно-техническую задачу в сфере профессиональной деятельности на основе знания проблем отрасли и опыта их решения	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-2	ИД-3ОПК-2	Владеет средствами анализа информационной безопасности.	Владеет навыками выбора методов решения, установления ограничений к решениям научно-технической задачи в сфере профессиональной деятельности на основе нормативно-технической документации и зна-ния проблем отрасли и опыта их решения	Защита лабораторной работы
ПКО-1	ИД-1ПКО-01	Знает: политику и стандарты безопасности; правовую и организационную поддержку процессов разработки и применения программного обеспечения.	Знает порядок выявления охраноспособных объектов, определения соответствия выявленных результатов интеллектуальной деятельности условиям патентоспособности: задачи, подлежащие решению, технический результат, новизна объекта, изобрета-тельский уровень, промышленная применимость и прочее	Дифференцированный зачет
ПКО-1	ИД-2ПКО-01	Умеет: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.	Умеет самостоятельно приобретать и использовать в практической деятельности знания в области интеллектуальной собственности, в том числе с помощью информационных технологий	Защита лабораторной работы
ПКО-1	ИД-3ПКО-01	Владеет средствами анализа информационной безопасности.	Владеет навыками сбора и анализа информации об уровне научно-технического развития в соответствующей профессиональной сфере - поиска, отбора и анализа научно-технической, патентной, правовой информации	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	72	72
- лекции (Л)	18	18
- лабораторные работы (ЛР)	24	24
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	26	26
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	72	72
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
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
4-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Понятие информационной безопасности	8	12	12	36
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. Защита от несанкционированного доступа: идентификация,				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
аутентификация, управление доступом. Алгоритмы аутентификации пользователей. Парольные системы аутентификации: идентификатор пользователя, пароль пользователя, учетная запись пользователя.				
Средства защиты информации	10	12	14	36
Тема 5. 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 6. 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 7. 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 8. 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				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
программного обеспечения.				
ИТОГО по 4-му семестру	18	24	26	72
ИТОГО по дисциплине	18	24	26	72

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Построение модели угроз безопасности информации.
2	Противодействие основным методам реализации угроз информационной безопасности.
3	Планирование развития компьютерной сети.
4	Мероприятия по обеспечению безопасности сети. Техническая поддержка пользователей сети.
5	Применение инкрементальных алгоритмов для защиты от вирусов.
6	Применение самотестирующихся и самокорректирующихся программ и их сочетаний.

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Исследование эффективности работы программных средств защиты от несанкционированного доступа.
2	Изучение основных средств безопасности Windows.
3	Анализ уязвимостей данных в ОС Windows и средств их устранения.
4	Анализ средств безопасности ASP.NET. Аутентификация.
5	Инсталляция и администрирование средств сетевой защиты распределенных хранилищ данных.
6	Криптопрограммирование с использованием стандартов DES и RSA.

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 приятия 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
1. Основная литература		
1	Семененко В.А. Информационная безопасность : учебное пособие / В.А.Семененко. - М.: Изд-во МГИУ, 2005.	10
2. Дополнительная литература		
2.1. Учебные и научные издания		

1	Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2007.	5
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
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)
Учебно-методическое обеспечение самостоятельной работы студентов	Безопасность и защита информации. Курс лекций.	ftp://itas.pstu.ru	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

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	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/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Персональные компьютеры.	20
Лекция	Мультимедийный проектор, экран.	1
Практическое занятие	Персональные компьютеры.	20

8. Фонд оценочных средств дисциплины

Описан в отдельном документе