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: Защита информации в компьютерных системах
(наименование)

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

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

Общая трудоёмкость: 180 (5)
(часы (ЗЕ))

Направление подготовки: 09.03.01 Информатика и вычислительная техника
(код и наименование направления)

Направленность: Информатика и вычислительная техника (общий профиль, СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель учебной дисциплины - получение знаний в области теоретических основ защиты информации и практических навыков в обеспечении защиты программного обеспечения.

Задачи учебной дисциплины:

- изучение основных методов и средств защиты информации;
- формирование умений в области технологии защиты программного обеспечения;
- формирование навыков, необходимых для разработки средств защиты программного обеспечения.

1.2. Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты:

- основные типы угроз информационной безопасности;
- основные способы от угроз;
- технические средства защиты;
- организационные и юридические мероприятия по обеспечению защиты информации;
- основы разработки средств защиты информации.

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-2.3	ИД-1ПК-2.3	Знает: - основные понятия и направления в защите программного обеспечения; - источники, риски, формы атак на информацию; - основные стандарты оценивания защищенности; - основные уязвимости программного обеспечения.	Знает средства защиты от несанкционированного доступа операционных систем и систем управления базами данных.	Экзамен

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.3	ИД-2ПК-2.3	Умеет: - инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения; - использовать парольные системы аутентификации; - применять средства и методы предотвращения вторжений.	Умеет конфигурировать сетевые устройства.	Защита лабораторной работы
ПК-2.3	ИД-3ПК-2.3	Осуществляет меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты. Устанавливает и настраивает программное обеспечение для защиты от вредоносного программного обеспечения.	Владеет навыками настройки параметров управления безопасностью операционных систем сетевых устройств.	Защита лабораторной работы

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: 1.1. Контактная аудиторная работа, из них:	44	44
- лекции (Л)	14	14
- лабораторные работы (ЛР)	28	28
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)		
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	100	100
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	180	180

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
6-й семестр				
Понятие информационной безопасности.	2	0	0	4
Основные понятия и определения.Система обработки информации. Объект информатизации. Информационные ресурсы. Защищаемая информация. Безопасность информации. Защиты информации. Парольная система. Техническая защита информации. Физическая защита информации. Способ защиты информации. Средство защиты информации.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Источники опасности для информации.	4	4	0	10
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.				
Средства защиты информации	4	16	0	54
Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом. Алгоритмы аутентификации пользователей. Парольные системы аутентификации: идентификатор пользователя, пароль пользователя, учетная запись пользователя. Установка и настройка сетевого программного обеспечения. Модернизация компьютерного оборудования. Мероприятия по обеспечению безопасности компьютерной сети сети. Техническая поддержка пользователей компьютерной сети. Защита от несанкционированного доступа: идентификация, аутентификация, управление доступом. Алгоритмы аутентификации пользователей. Парольные системы аутентификации: идентификатор пользователя, пароль пользователя, учетная запись пользователя.				
Криптографическая защита информации	4	8	0	32
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. Методы обеспечения надежности программ, используемые для контроля технологической безопасности. Самотестирующиеся и самокорректирующиеся программы. Общие принципы создания двухмодульных вычислительных процедур и методология самотестирования. Исследования процесса верификации расчетных программ. Области применения самотестирующихся и				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
самокорректирующихся программ и их сочетаний.				
ИТОГО по 6-му семестру	14	28	0	100
ИТОГО по дисциплине	14	28	0	100

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Анализ программных средств защиты от несанкционированного доступа
2	Анализ средств безопасности операционной системы
3	Анализ уязвимостей данных в операционной системе
4	Анализ средств безопасности ASP.NET. Аутентификация
5	Анализ средств защиты баз данных
6	Шифрование информации с использованием стандартов DES и RSA
7	Алгоритмы хеширование паролей
8	Шифрование методом гаммирования

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.

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 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	Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. - М.: Радио и связь, 2001.	11
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов. - Москва: Проспект, 2010.	4
2	Мельников В. П. Защита информации : учебник для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - Москва: Академия, 2014.	6
3	Семененко В.А. Информационная безопасность : учебное пособие для вузов / В.А. Семененко. - М.: Изд-во МГИУ, 2006.	10
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)
Дополнительная литература	Защита информации и информационная безопасность	https://znanium.com/read?id=366835	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	Debian (GNU GPL)
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	LibreOffice 6.2.4. OpenSource, бесплатен.
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
База данных научной электронной библиотеки (eLIBRARY.RU)	https://elibrary.ru/
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/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	персональный компьютер	30
Лекция	персональный компьютер (ноутбук), мультипроектор, экран	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»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине
«Защита информации в компьютерных системах»
Приложение к рабочей программе дисциплины

Направление подготовки:	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы:	Информатика и вычислительная техника (общий профиль, СУОС)
Квалификация выпускника:	«Бакалавр»
Выпускающая кафедра:	Информационных технологий и автоматизированных систем (ИТАС)
Форма обучения:	Очная

Курс: 3 Семестр: 6

Трудоёмкость:
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч.

Форма промежуточной аттестации:
Экзамен: 6 семестр

Пермь 2023 г.

Фонд оценочных средств 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 (6-го семестра учебного плана). Согласно РПД 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 (таблица 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		**Промежуточный /рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 знать средства защиты от несанкционированного доступа операционных систем и систем управления базами данных		ТО1				ТВ
Освоенные умения						
У.1 уметь конфигурировать сетевые устройства			ОЛР1			ПЗ
Приобретенные владения						
В.1 владеть навыками настройки параметров управления безопасностью операционных систем сетевых устройств			ОЛР2			КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос);КЗ – кейс-задача (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 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 (промежуточный) контроль

Рубежный (промежуточный) контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (таблица 1.1) проводится в форме защиты лабораторных работ.

2.2.1. Защита лабораторных работ

Всего запланировано 8 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом или группой студентов. 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, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений 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. Классификация угроз информационной безопасности: для личности, для общества, для государства.
2. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
3. Элементы и объекты защиты в автоматизированных системах обработки данных.
4. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
5. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
6. Электронная (цифровая) подпись. Цели применения электронной подписи.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Определение объектов защиты на типовом объекте информатизации (по вариантам).
2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности (по вариантам).
3. Понятие и подходы к построению модели угроз.
4. Виды и каналы утечки информации (по вариантам).
5. Основные методы реализации угроз информационной безопасности (по вариантам).
6. На основе ГОСТ Р ИСО/МЭК 17799-2005, и с точки зрения начальника отдела по вопросам информационной безопасности в небольшой организации разработать перечень мероприятий при привлечении сторонних организаций к обработке информации.

Типовые комплексные задания для контроля приобретенных владений:

1. Произвести оценку доступности компьютера вашего рабочего места для сетевых атак с точки зрения открытых для атак портов. Дать оценку полученным результатам.

2. Произвести оценку открытости для сетевых атак заданного сайта. Узнать его IP - адрес, владельца сайта, дату регистрацию домена, оплату домена, используемое ПО (CMS). Дать оценку полученным результатам.

3. Произвести определение настроек браузера вашего компьютера, влияющих на безопасности работы в сети Интернет, а также актуальность браузера. Дать оценку полученным результатам и рекомендации по улучшению настроек.

Полный перечень теоретических вопросов и практических заданий в форме утвержденного комплекта экзаменационных билетов хранится на выпускающей кафедре.

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.