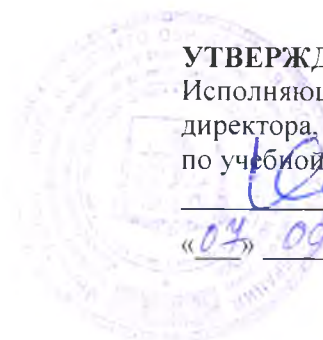


Министерство науки и высшего образования Российской Федерации
Чайковский филиал
федерального государственного бюджетного образовательного учреждения
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**



УТВЕРЖДАЮ

Исполняющий обязанности
директора, заместитель директора
по учебной работе ЧФ ПНИПУ
_____ Н. М. Куликов

«04» _____ 2020 г.

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

Направление подготовки: 09.03.01 «Информатика и вычислительная техника»

Направленность (профиль) образовательной программы: Автоматизированные системы обработки информации и управления

Квалификация выпускника: «бакалавр»

Выпускающая кафедра: кафедра автоматизации, информационных и инженерных технологий

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.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины «**Защита информации**». 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-ый семестр учебного плана) и состоит из одного учебного модуля. В процессе изучения дисциплины предусмотрено проведение лекционных и лабораторных занятий, а также выполнение самостоятельной работы студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций знать, уметь, владеть, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, выполнении лабораторных работ, индивидуальных заданий и сдаче экзамена. Виды контроля сведены в табл. 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					
3.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. Современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	С	ТО	ОЛР		ТВ
3.2 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		ТО	ОЛР		ТВ

Освоенные умения					
У.1 Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.				ОЛР	ПЗ
У.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности				ОЛР	ПЗ
Приобретенные владения					
В.1 Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.				ОЛР	ПЗ
В.2 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научноисследовательской работе с учетом требований информационной безопасности.					ПЗ

С – собеседование по теме; ТО – теоретический опрос; ИЗ – индивидуальное задание; ОЛР – отчет по лабораторной работе; Т – рубежное тестирование; ТВ – теоретический вопрос экзамена; ПЗ – практическое 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 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 работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам. Рубежный контроль по дисциплине проводится за неделю до окончания дисциплины, а промежуточный – после прохождения каждой из 8 тем дисциплины в форме сдачи отчета по лабораторной работе;

– 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 опроса и анализа усвоения материала предыдущей лекции, 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, усвоенных умений и приобретенных владений проводится в форме защиты лабораторных работ.

2.2.1. Защита лабораторных работ

Всего запланировано 7 лабораторных работ. Типовые темы лабораторных работ:

1. Анализ программных средств защиты от несанкционированного доступа.
2. Анализ средств безопасности операционной системы.
3. Проектирование средств физической защиты данных
4. Самотестирующиеся и самокорректирующиеся программы.
5. Шифрование информации с использованием стандарта DES и RSA
6. Построения симметричных криптосистем. Классические разновидности шифров.
7. Алгоритмы сжатия информации

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

Методические предписания к выполнению лабораторных работ и фонды типовых заданий на лабораторные работы включены в состав УМКД на правах отдельных документов. Примеры типовых заданий на лабораторные работы представлены в Приложении 1 данного документа.

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 форме экзамена.

2.3.1. Порядок организации экзамена по дисциплине

Экзамен по дисциплине «Защита информации» проводится по экзаменационным билетам, в устной форме. Экзаменационный билет содержит два теоретических вопроса (для проверки усвоения знаний) и одну задачу (для проверки освоенных умений). Уровень приобретенных владений оценивается по результатам выполнения и защиты лабораторных работ, индивидуальных заданий. Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности всех заявленных компетенций.

Форма билета для экзамена представлена в Приложении 2.

2.3.1.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Проблемы защиты информации и подходы к ее решению
2. Основные понятия защиты информации
3. Угрозы безопасности и каналы утечки информации
4. Классификация методов и средств защиты информации
5. Правовое обеспечение защиты информации
6. Безопасность программного обеспечения и человеческий фактор
7. Способы аутентификации пользователей на основе паролей
8. Программно-аппаратная защита от несанкционированного доступа
9. Методы физической защиты от несанкционированного доступа
10. Организационные методы защиты от несанкционированного доступа
11. Аутентификация пользователей на основе их биометрических характеристик
12. Избирательное, мандатное и ролевое разграничение доступа к объектам.
13. Криптопрограммирование. использования инкрементальных алгоритмов
14. Криптографические модели Классификация криптоалгоритмов
15. Криптографические модели Симметричные криптоалгоритмы.
Скремблеры
16. Виды Хеш-функций. Метод деления. Метод умножения (мультипликативный) метод
17. Виды Хеш-функций. Виды Хеш-функций. Динамическое хеширование.
18. Виды Хеш-функций. Расширяемое хеширование. (extendible hashing)
19. Минимальное идеальное хеширование. Разрешение коллизий.
20. Разрешение коллизий. Метод цепочек.
21. Разрешение коллизий. Линейная адресация.

22. Разрешение коллизий. Квадратичная и произвольная адресация.
23. Разрешение коллизий. Адресация с двойным хешированием (рехеширование)
24. Хеширование паролей с линейный конгруэнтным генератором.
25. Хеширование паролей с генератором Парка-Миллера
26. Хеширование паролей с генератором Геффа
27. Хеширование паролей с аддитивным генератором
28. Электронная цифровая подписью и ее применение

Практическое задание для контроля освоенных умений может быть предложено по следующим темам:

1. Средства администрирования подсистемы информационной безопасности и объекта защиты
2. Политика безопасности стандарты безопасности
3. Криптографическая защита информации
4. Само тестирующиеся и самокорректирующиеся программы

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

2.3.1.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине «Защита информации» 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 дисциплинарных 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.

Типовые задания на лабораторные работы для проверки умений и владений

Лабораторная работа 1.

Реферат на тему Анализ средств защиты от несанкционированного доступа

Лабораторная работа № 2

Проектирование средств физической защиты даннь

Цель работы: изучить основные методы организации физической защиты данных
Для выполнения лабораторной работы, требуется разработать технологические и организационные мероприятия защиты данных

Лабораторная работа № 3

Создание симметричных криптоалгоритмов методом перестановки.

Цель работы: Умение создавать симметричные криптоалгоритмы методом перестановки.

Лабораторная работа № 4

Методы криптографического закрытия. Гаммирование.

Цель работы: Умение создавать симметричные криптоалгоритмы применяя методы гаммирования.

Лабораторная работа № 5

Помехоустойчивое кодирование

Цель работы: Исследование принципов помехоустойчивого кодирования на примере корректирующих кодов Хемминга.

Для выполнения лабораторной работы, требуется изучить логику и пошаговое действие алгоритма Хэмминга.

Методом Хемминга закодировать указанные информационные комбинации, построив порождающую проверочную матрицы. Внести ошибку в один из разрядов кодового вектора; найти синдром; найти и исправить ошибку.

Лабораторная работа № 6

Работа с таблицей символов

Цель работы: изучить основные методы организации таблиц идентификаторов, получить представление о преимуществах и недостатках, присущих различным методам организации таблиц символов (идентификаторов).

Для выполнения лабораторной работы требуется написать программу, которая получает на входе набор идентификаторов, организует таблицу по заданному методу и позволяет осуществить многократный поиск идентификатора в этой таблице. Список идентификаторов считать заданным в виде текстового файла. Длина идентификаторов ограничена 32 символами.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Хеширование паролей с линейным конгруэнтным генератором.
2. Избирательное, мандатное и ролевое разграничение доступа к объектам.
3. Индивидуальное задание . Вариант1

« _____ » _____ 20__ г.

Зав. кафедрой _____