МИНОБРНАУКИ РОССИИ
Воткинский филиал
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ

Директор

_____/Давыдов И.А.

01 апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: очная

общая трудоемкость дисциплины составляет: 3 зачетных единиц(ы)

Кафедра Естественные науки и информационные технологии

Составитель _____

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования и рассмотрена на заседании кафедры

Протокол от __01 апреля_ 2022 г. № __2___

Заведующий кафедрой _____К.Б. Сентяков

_____ 2022г.

СОГЛАСОВАНО

Количество часов рабочей программы и формируемые компетенции соответствуют учебному плану направления 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

Председатель учебно-методической комиссии по направлению 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

_____К.Б. Сентяков

_____ 2022 г.

Руководитель образовательной программы

_____ К.Б. Сентяков

_____ 2022 г.

Аннотация к дисциплине

Название дисциплины	Защита информации
Направление подготовки (специальность)	09.03.01 «Информатика и вычислительная техника»
Направленность (профиль/программа/специализация)	Автоматизированные системы обработки информации и управления
Место дисциплины	Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».
Трудоемкость (з.е. / часы)	3 з.е. / 108 часов
Цель изучения дисциплины	Формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности
Компетенции, формируемые в результате освоения дисциплины	ПК-8 Способен участвовать в разработке и эксплуатации защищенных автоматизированных систем.
Содержание дисциплины (основные разделы и темы)	Требования к построению защищенных информационных систем. Анализ угроз информационной безопасности и методология построения систем защиты информации Комплексный подход к обеспечению информационной безопасности Технологии обеспечения безопасности информации в автоматизированных системах
Форма промежуточной аттестации	Зачет (8 сем)

1.Цели и задачи дисциплины:

Целью освоения дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности

Задачи дисциплины:

- изучение методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

- изучение методов и требований к программно- аппаратной защите информации;

- получение навыков выбора средств защиты и их применения в автоматизированных системах

2. Планируемые результаты обучения

В результате освоения дисциплины у студента должны быть сформированы

Знания, приобретаемые в ходе освоения дисциплины

№ п/п	Знания
1	Требований к построению защищенных информационных систем
2	Классификации угроз информационной безопасности
3	Основных принципов и методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

Умения, приобретаемые в ходе освоения дисциплины

№ п/п	Умения
1	Классификации автоматизированных систем с позиции обеспечения информационной безопасности
2	Выбора базового набора методов и средств защиты автоматизированной системы

Навыки, приобретаемые в ходе освоения дисциплины

№ п/п	Навыки
1	Навыки применения средств защиты информации в автоматизированных системах

Компетенции, приобретаемые в ходе освоения дисциплины

Компетенции	Индикаторы	Знания	Умения	Навыки
ПК-8 Способен участвовать в разработке и эксплуатации защищенных автоматизированных систем	ПК-8.1: Знать: современные угрозы информационной безопасности, методы и средства обеспечения безопасности в автоматизированных системах	1,2,3		
	ПК-8.2: Уметь: проводить классификацию автомат изированных систем и определять требования к построению защищенных автоматизированных систем		1,2	
	ПК-8.3: Владеть: навыками применения методов обеспечения информационной безопасности автоматизированных систем			1

3. Место дисциплины в структуре ООП

Дисциплина относится к Блоку 1.Дисциплины «Защита информации». Части, формируемая участниками образовательных отношений Дисциплина изучается на 4 курсе в 8 семестре.

Изучение дисциплины базируется на знаниях, умениях и навыках, полученных при освоении дисциплин «Защита информации»: Правовые основы информационной безопасности, Программирование, Базы данных, Операционные системы, Сети и телекоммуникации

Перечень последующих дисциплин (модулей), для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной (модулем): Проектирование автоматизированных систем обработки информации и управления

4. Структура и содержание дисциплины

4.1 Структура дисциплин

№ п/п	Раздел дисциплины. Форма промежуточной аттестации *(по семестрам)*	Всего часов раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы					Содержание самостоятельной работы
				контактная				СРС	
				лек	пр	лаб	КЧА		
1	2	3	4	5	6	7	8	10	11
1	Введение. Требования к построению защищенных информационных систем	15	8	1	2	2		10	[1,2] Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №1, ответам на вопросы при сдаче лабораторной работы
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	26	8	6	8	2		10	[1,2] Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №2, ответам на вопросы при сдаче лабораторной работы
3	Комплексный подход к обеспечению информационной безопасности	24	8	3	6	-		15	[1,2] Практическая работа. Подготовка к вопросам по практической работе

4	Технологии обеспечения безопасности информации в автоматизированных системах	41	8	2	8	8		23	[1,2] Подготовка к устному опросу Практическая работа. Подготовка к вопросам по практической работе Подготовка к выполнению лабораторной работы №3,4, ответам на вопросы при сдаче лабораторной работы
	Зачет	2		–	–	–	0,3	1,7	Зачет выставляется по совокупности результатов текущего контроля успеваемости или проводится в письменной форме
	Итого:	**108**		**12**	**24**	**12**	**0,3**	**59,7**	

4.2 Содержание разделов курса и формируемых в них компетенций

№ п/п	Раздел дисциплины	Коды компетенции и индикаторов	Знания	Умения	Навыки	Форма контроля
1	Введение. Требования к построению защищенных информационных систем	ПК 8.1, ПК 8.2	1	1,2	1	Практическая работа Выполнение лабораторной работы №1, ответ на вопросы при сдаче работы
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	ПК 8.1, ПК 8.2	2,3	1,2	1	Выполнение лабораторной работы №2, ответ на вопросы при сдаче работы Практическая работа
3	Комплексный подход к обеспечению информационной безопасности	ПК 8.1, ПК 8.2, ПК 8.3	2,3	1,2	1	Практическая работа
4	Технологии обеспечения безопасности информации в автоматизированных системах	ПК 8.2, ПК 8.3	2,3	1,2	1	Устный опрос Практическая работа Выполнение лабораторной работы№3-4, ответ на вопросы при сдаче работы

4.3 Наименование тем лекций, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование лекций	Трудоемкость(час)
1.	1	Классификация информационных систем по требованиям безопасности	0,5
2.	1	Требования к построению защищенных информационных систем	0,5
3.	2	Анализ угроз информационной безопасности	1
4.	2	Каналы утечки информации. Классификация компьютерных вирусов	1

5.	2	Основные принципы обеспечения информационной безопасности. Методы и инструменты обеспечения информационной безопасности. Политика информационной безопасности	1
6.	2	Методы разграничения доступа к информации. Матрица доступа.	1
7.	2	Стандарты информационной безопасности.	1
8.	2	Лицензирование, сертификация в области информационной безопасности. Понятие аттестации объектов информатизации	1
9.	3	Криптографические методы защиты информации. Симметричные и ассиметричные системы шифрования	2
10	3	Общая характеристика и классификация мер и средств защиты информации от НСД	1
11	4	Технологии аутентификации. Протокол Kerberos.	1
12	4	Электронная подпись и функция хэширования.Стандарты цифровой подписи	1
	Всего		**12**

4.4 Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоем-кость (час)
1.	1	Классификация информационных систем. Классификация информационных систем персональных данных (ИСПДН).Анализ базовых требований к защите ИСПДН.	1
2.	1	Классификация государственных информационных систем (ГИС). Требования к защите ГИС	1
3.	2	Анализ требований отечественных и международных стандартов информационной безопасности	2
4.	2	Политика безопасности предприятия	4
5.	2	Анализ и подбор сертифицированных средств защиты информации	2
6.	3	Криптографические алгоритмы защиты информации.	6
7.	4	Алгоритм цифровой подписи. Алгоритмы хэш-функций. Стандарты РФ на криптографические алгоритмы	2
8.	4	Программно-аппаратные средства защиты от НСД	6
	Всего		**24**

4.5 Наименование тем лабораторных работ, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Трудоем-кость (час)
1.	1	Классификация информационным системам персональных данных. Набор базовых метод по защите персональных данных	2
2.	2	Компьютерные вирусы. Макровирусы	2
3.	4	Программно-аппаратные средства защиты данных	4
4.	4	Цифровые сертификаты. Установка, настройка программного обеспечения криптопровайдеров.	4
	Всего		**12**

5. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации подисциплине

- вопросы для устного опроса
- защиты лабораторных работ;
- зачет

Примечание: оценочные материалы (типовые варианты тестов, контрольных работ и др.) приведены в приложении к рабочей программе дисциплины.

Промежуточная аттестация по итогам освоения дисциплины – зачет

6. Учебно-методическое и информационное обеспечение дисциплины:

1. а) Основная литература

№ п/п	Наименование книги	Год издания
1	Нестеров С.А., Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html	2014

б) Дополнительная литература

№ п/п	Наименование книги	Год издания
2	Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю. Н. Сычев. — Электрон. текстовые данные. — Саратов : Вузовское образование, 2018. — 195 c. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html	2018

в) перечень ресурсов информационно-коммуникационной сети Интернет

1. Электронно-библиотечная система IPRbooks http://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова Web ИРБИС http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN=IBIS
3. Национальная электронная библиотека - http://нэб.рф
4. Мировая цифровая библиотека - http://www.wdl.org/ru
5. Международный индекс научного цитирования Web of Science - http://webofscience.com
6. Научная электронная библиотека eLIBRARY.RU – https://elibrary.ru/defaultx.asp

г) программное обеспечение:

1. LibreOffice
2. Doctor Web Enterprise Suite
3. PGP

д) методические указания:

1. Алексеев, В. А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / В. А. Алексеев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — ISBN 2227-8397.

— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.html

2. Бурняшов, Б. А. Меры защиты информации на уровне пользователя информационно-технологическими средствами : методические указания к самостоятельной работе студентов. Учебно-методическое пособие / Б. А. Бурняшов. — Саратов : Вузовское образование, 2014. — 55 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/23077.html

7. Материально-техническое обеспечение дисциплины:

1. Лекционные занятия.

Учебные аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

2. Практические занятия.

Учебные аудитории для практических занятий укомплектованы специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук).

3. Лабораторные работы.

Для лабораторных занятий используются аудитории:

№ 220 адрес: 427430, Удмуртская Республика, г. Воткинск, ул. П.И. Шувалова, д. 1, оснащенная следующим оборудованием: столы лабораторные, стулья, компьютерная техника с возможностью подключения к сети «Интернет».

№ 221 адрес: 427430, Удмуртская Республика, г. Воткинск, ул. П.И. Шувалова, д. 1, оснащенная следующим оборудованием: столы лабораторные, стулья, компьютерная техника с возможностью подключения к сети «Интернет».

4. Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»:

помещения для самостоятельной работы обучающихся (ауд.№ 224, адрес: 427430, Удмуртская Республика, г. Воткинск, ул. П.И. Шувалова, д. 1).

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

Лист согласования рабочей программы дисциплины на учебный год

Рабочая программа дисциплины (модуля) «Защита информации» по направлению подготовки 09.03.01 «Информатика и вычислительная техника»
по профилю «Автоматизированные системы обработки информации и управления»

согласована на ведение учебного процесса в учебном году:

Учебный год	***«Согласовано»:*** *заведующий кафедрой, ответственной за РПД (подпись и дата)*
2021 – 2022	
2022 – 2023	
2023 – 2024	
2024 – 2025	

Приложение к рабочей программе дисциплины

МИНОБРНАУКИ РОССИИ
Воткинский филиал
Федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

Оценочные средства по дисциплине

Защита информации

направление 09.03.01 «Информатика и вычислительная техника»

профиль «Автоматизированные системы обработки информации и управления»

уровень образования: бакалавриат

форма обучения: очная

общая трудоемкость дисциплины составляет: 3 зачетных единиц(ы)

1.Оценочные средства

Оценивание формирования компетенций производится на основе результатов обучения, приведенных в п. 2 рабочей программы и ФОС. Связь разделов компетенций, индикаторов и форм контроля (текущего и промежуточного) указаны в таблице 4.2 рабочей программы дисциплины.

Оценочные средства соотнесены с результатами обучения по дисциплине и индикаторами достижения компетенций, представлены ниже.

№ п/п	Коды компетенции и индикаторов	Результат обучения *(знания, умения и навыки)*	Формы текущего и промежуточного контроля
1	ПК-8.1: Знать: современные угрозы информационной безопасности, методы и средства обеспечения безопасности в автоматизированных системах	З1.Требований к построению защищенных информационных систем У1.Классификации автоматизированных систем с позиции обеспечения информационной безопасности У2.Выбора базового набора методов и средств защиты автоматизированной системы Н1.Навыки применения средств защиты информации в автоматизированных системах	Ответ на вопросы по практической работе , защита лабораторной работы №1,2 зачет
2	ПК-8.2: Уметь: выявлять уязвимые места в автоматизированных системах с точки зрения информационной безопасности, применять методы и средства защиты данных	З2.Классификации угроз информационной безопасности З3.Основных принципов и методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы У1. Классификации автоматизированных систем с позиции обеспечения информационной безопасности У2.Выбора базового набора методов и средств защиты автоматизированной системы Н1.Навыки применения средств защиты информации в автоматизированных системах	Ответ на вопросы по практической работе , защита лабораторной работы №1,2,3,4, устный опрос, зачет
3	ПК-8.3: Владеть: навыками администрирования автоматизированных систем с у четом требований информационной безопасности	З2. Классификации угроз информационной безопасности З3.Основных принципов и методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы У1. Классификации автоматизированных систем с позиции обеспечения информационной безопасности У2.Выбора базового набора методов и средств защиты автоматизированной системы Н1.Навыки применения средств защиты информации в автоматизированных системах	Ответ на вопросы по практической работе , защита лабораторной работы №3,4, устный опрос, зачет

Типовые задания для оценивания формирования компетенций

Наименование: зачет
Представление в ФОС:
Перечень вопросов для проведения зачета:

1. Понятие «информационной безопасности». Составляющие информационной безопасности. Классификация методов защиты информации. Организации - регуляторы в области ИБ.
2. Законодательство в области защиты персональных данных. Категории персональных данных. Специальная категория данных. Угрозы 1,2,3 типа при классификации персональных данных. Какая информация должна содержаться в согласии субъекта на обработку персональных данных.
3. Угрозы ИБ. Каналы утечки информации.
4. Понятие модели угроз. Модели угроз для информационных систем персональных данных. (Примеры)
5. Классификация компьютерных вирусов по деструктивным возможностям.
6. Виды "вирусоподобных" программ. Поясните механизм функционирования "троянской программы", «логической бомбы», макровируса
7. Классификация криптографических систем. Назовите наиболее известные криптографические отечественные и зарубежные алгоритмы и дайте им краткую характеристику.
8. Матрица доступа принципы составления. Примеры
9. Анализ рисков информационной безопасности. Методики и программные продукты для оценки рисков
10. Принципы реализации симметричного метода шифрования
11. Принципы реализации асимметричного метода шифрования
12. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
13. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
14. Биометрические средства идентификации и аутентификации пользователей.
15. Аутентификация субъектов в распределенных системах. Метод одноразовых паролей, метод рукопожатия
16. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
17. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
18. Законодательный уровень применения цифровой подписи. Понятие и применение сертификата.

Критерии оценки:
Приведены в разделе 2

Наименование: защита лабораторных работ
Представление в ФОС*:** задания и требования к выполнению представлены в методических указаниях по дисциплине ***Варианты заданий:
задания и требования к выполнению представлены в методических указаниях по дисциплине
Критерии оценки:
Приведены в разделе 2

Наименование: устный опрос

***Представление в ФОС*:** перечень заданий или вопросов
Варианты заданий:

- Перечислите проблемы парольной аутентификации
- Опишите алгоритм аутентификации сервера на основе одноразовых паролей
- Опишите основную идею алгоритма аутентификации Kerberos ***Критерии оценки:***

Приведены в разделе 2

Наименование: практические работы
Представление в ФОС*:** набор вариантов заданий ***Варианты заданий:

- Перечислите законодательство в области защиты персональных данных
- Дайте определение и приведите примеры "Объектов критической инфраструктуры"
- Опишите роль следующих организаций в области ЗИ: ФСТЭК, ФСБ, АНБ
- Провести анализ уязвимостей MS OFFICE. Макровирусы среда распространения и методы защиты
- Найти и проанализировать методические документы на сайте регулятора ИБ www.fstec.ru.
- Опишите назначение и приведите примеры программно-аппаратных средств защиты информации

Критерии оценки:
Приведены в разделе 2

2.Критерии и шкалы оценивания

Для контрольных мероприятий (текущего контроля) устанавливается минимальное и максимальное количество баллов в соответствии с таблицей. Контрольное мероприятие считается пройденным успешно при условии набора количества баллов не ниже минимального.

Результат обучения по дисциплине считается достигнутым при успешном прохождении обучающимся всех контрольных мероприятий, относящихся к данному результату обучения.

Разделы дисциплины	***Форма контроля***	***Количество баллов***	
		min	***max***
1	Выполнение практической работы, ответ на вопросы	2	5
1	Выполнение практической работы, ответ на вопросы	2	5
1	Выполнение лабораторной работы №1, ответ на вопросы	8	12
2	Выполнение практической работы, ответ на вопросы	2	5
2	Выполнение практической работы, ответ на вопросы	2	5
2	Выполнение практической работы, ответ на вопросы	2	5
2	Выполнение лабораторной работы №2, ответ на вопросы	8	12
3	Выполнение практической работы, ответ на вопросы	3	5
4	Выполнение практической работы, ответ на вопросы	3	5
4	Выполнение практической работы, ответ на вопросы	3	5
4	Выполнение лабораторной работы №3, ответ на вопросы	8	12
4	Выполнение лабораторной работы №4, ответ на вопросы	8	12
4	Устный опрос	9	12
	Итого	**60**	**100**

При оценивании результатов обучения по дисциплине в ходе текущего контроля успеваемости используются следующие критерии. Минимальное количество баллов выставляется обучающемуся при выполнении всех показателей, допускаются несущественные неточности в изложении и оформлении материала.

Наименование, обозначение	***Показатели выставления минимального количества баллов***
Практическая работа	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий. На защите практической работы даны правильные ответы не менее чем на 50% заданных вопросов
Лабораторная работа	Лабораторная работа выполнена в полном объеме; Продемонстрирован удовлетворительный уровень владения материалом при защите лабораторной работы, даны правильные ответы не менее чем на 50% заданных вопросов
Устный опрос	Даны правильные ответы не менее чем на 50% заданных вопросов. Продемонстрированы знания основного учебно-программного материала

Промежуточная аттестация по дисциплине проводится в форме зачета.

Итоговая оценка по дисциплине может быть выставлена на основе результатов текущего контроля с использованием следующей шкалы:

Оценка	***Набрано баллов***
«зачтено»	60-100
«не зачтено»	Менее 60

Если сумма набранных баллов менее 60 – обучающийся не допускается до промежуточной аттестации.

Если сумма баллов составляет от 60_ до 100 баллов, обучающийся допускается до зачета.

При оценивании результатов обучения по дисциплине в ходе промежуточной аттестации используются следующие критерии и шкала оценки:

Оценка	***Критерии оценки***
«зачтено»	Обучающийся демонстрирует знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы, умеет применять его при выполнении конкретных заданий, предусмотренных программой дисциплины
«не зачтено»	Обучающийся демонстрирует значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение