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.
__03__июня__2020_ 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 __03__июня___ 2020 г. №__4__

Заведующий кафедрой _____К.Б. Сентяков

__03__июня___ 2020 г.

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

__03__июня___ 2020 г.

Руководитель образовательной программы _____ К.Б. Сентяков

__03__июня___ 2020 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	Блока 1 Часть, формируемая участниками образовательных отношений
Трудоемкость (з.е. / часы)	3 з.е./ 108 часов
Цель изучения дисциплины	**Целью** преподавания дисциплины является формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности
Компетенции, формируемые в результате освоения дисциплины	**ПК-8** Способен обеспечивать информационную безопасность уровня баз данных
Содержание дисциплины (основные разделы и темы)	- Введение. Информационная безопасность: основные понятия и определения - 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

1. Цели и задачи дисциплины:

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

Задачи дисциплины:

- изучение организационно - правовых основ информационной безопасности;
- изучение криптографических средств защиты информации;
- изучение методов и требований к программно- аппаратной защите информации;
- изучение методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

В результате изучения дисциплины студент должен

знать:

- политику безопасности РФ в области информационной безопасности
- основные угрозы и каналы утечки информации;
- методы комплексного обеспечения информационной безопасности

уметь:

- составлять содержание и план работы в профессиональной области с учетом требований информационной безопасности

владеть:

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

2. Место дисциплины в структуре ООП:

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».

Для изучения дисциплины студент должен

знать:

- основные компоненты ПК и их технические характеристики;
- основное назначение прикладных, системных и служебных программ;
- этапы жизненного цикла информационных систем

уметь:

- пользоваться антивирусными программами;

владеть:

- навыками работы с офисными приложениями
- навыками программирования на языках высокого уровня

Изучение дисциплины базируется на знаниях, полученных при изучении дисциплин: Информатика, Программирование, Информационные системы

3. Требования к результатам освоения дисциплины

3.1. Знания, приобретаемые в ходе изучения дисциплины

№ п/п З	Знания
1.	политики безопасности РФ в области информационной безопасности
2.	основных угроз и каналов утечки информации;
3.	методов комплексного обеспечения информационной безопасности

3.2. Умения, приобретаемые в ходе изучения дисциплины

№ п/п У	Умения
1.	составлять содержание и план работы в профессиональной области с учетом требований информационной безопасности

3.3. Навыки, приобретаемые в ходе изучения дисциплины

№ п/п	Навыки
1.	навыки применения методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы

3.4.Компетенции, приобретаемые в ходе изучения дисциплины

Компетенции	Индикаторы	Знания (№№ из 3.1)	Умения №№ из 3.2)	Навыки (№№ из 3.3)
ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	ПК-8.1 Знать: современные угрозы информационной безопасности, методы и средства обеспечения безопасности в информационных системах и базах данных. ПК-8.2 Уметь: выявлять уязвимые места в информационных системах и базах данных с точки зрения информационной безопасности, применять методы и средства защиты данных. ПК-8.3 Владеть: навыками администрирования баз данных	1,2,3	1	1

4. Структура и содержание дисциплины

4.1. Разделы дисциплин и виды занятий

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, самостоятельная работа студентов и трудоемкость (в часах))				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				лек	*прак*	*лаб*	*СРС**	
1	Введение. Информационная безопасность: основные понятия и определения	8	1 2	2	4		8	работа на практических занятиях; Подготовка к зачету
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	8	3 4 5 6	4	8	2	12	работа на практических и лабораторных занятиях; Подготовка к зачету

3	Комплексный подход к обеспечению информационной безопасности	8	7 8	2	4		12	работа на практических занятиях; Подготовка к зачету
4	Технологии обеспечения безопасности информации в автоматизированных системах	8	9 10 11 12	4	8	10	26	работа на практических и лабораторных занятиях; защита лабораторной работы. Подготовка к зачету
							2	Зачет
	Всего			12	24	12	60	
	В том числе контроль самостоятельной работы				2			

***включая курсовое проектирование**

4.2. Содержание разделов курса

№ п/п	Раздел Дисциплины	Знания (номер из 3.1)	Умения (номер из 3.2)	Навыки (номер из 3.3)
1	1. Цели и задачи курса. Основные понятия и определения. Национальные интересы и безопасность России. Информация ограниченного доступа. Виды защищаемой информации. 2. Составляющие информационной безопасности. Основные принципы обеспечения информационной безопасности. Методы и инструменты обеспечения информационной безопасности 3. Нормативно-правовое регулирование в области защиты информации	1,3	1	1
2	1. Угрозы информационной безопасности и каналы утечки информации 2. Классификация компьютерных вирусов 3. Стандарты информационной безопасности 4. Методы разграничения доступа к информации 5. Политика информационной безопасности. 6. Лицензирование, сертификация в области информационной безопасности 7. Анализ рисков информационной безопасности	1,2,3	1	1

3	1. Организационно правовое обеспечение информационной безопасности. 2. Криптографические методы защиты информации. Симметричные, ассиметричные шифры. 3. Программно – технические методы и средства обеспечения ИБ	1,3	1	1
4	1. Идентификация и аутентификация. Протокол Kerberos. 2. Функции хэширования. 3. Цифровая подпись. Стандарты цифровой подписи.	1,3	1	1

4.3. Наименование тем практических занятий, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических работ	Трудоемкость (час)
1.	**1**	Национальные интересы РФ в области ИБ, приоритетные направления в области защиты информации. Органы, обеспечивающие национальную безопасность РФ	**2**
2.	**1**	Виды информации. Правовое обеспечение защиты информации. Классификация информационных систем персональных данных	**2**
3.	**2**	Угрозы ИБ. Понятие модели угроз. Модель злоумышленника.	**2**
4	**2**	Стандарты информационной безопасности.	**2**
5	**2**	Политика безопасности предприятия	**2**
6	**2,3**	Составление матрицы доступа. Анализ и подбор сертифицированных средств защиты информации	**4**
7	**3**	Криптографические алгоритмы защиты информации.	**2**
8	**4**	Алгоритм цифровой подписи. Алгоритмы хэш-функций. Стандарты РФ на криптографические алгоритмы	**8**
	Всего		**24**

4.4.Наименование тем лабораторных работ, их содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Трудоемкость (час)
1.	2	Макровирусы	**2**
2.	4	Программно-аппаратные средства защиты данных. Виды информации ограниченного доступа. Классификация и требования нормативных документов к информационным системам персональных данных.	**6**
3.	4	Цифровые сертификаты. Установка, настройка программного обеспечения криптопровайдеров.	**4**
	Всего		**12**

5. Содержание самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Содержание самостоятельной работы

№ п/п	№ раздела дисциплины	Наименование тем	Трудоем-кость (час)
1.	1	Проблема информационной безопасности в сфере государственного и муниципального управления	8
2.	2	Модель нарушителя информационных систем	3
3	2	Классификация компьютерных вирусов и методов защиты информации	3
4	2	Системы обнаружения вторжений. Инциденты информационной безопасности.	3
5	2	Методики и программные продукты для оценки рисков	3
6	3	Криптографические алгоритмы защиты информации	12
7	4	Инфраструктура открытых ключей . Цифровые сертификаты	26
		Зачет	2
	Всего		60

5.2. Оценочные средства, используемые для текущего контроля успеваемости и промежуточной аттестации обучающихся по итогам освоения дисциплины, их виды и формы, требования к ним и шкалы оценивания приведены в приложении к рабочей программе дисциплины «Фонд оценочных средств по дисциплине «Защита информации», которое оформляется в виде отдельного документа.

6. Учебно-методическое и информационное обеспечение дисциплины:

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. Специальные помещения - учебные аудитории для проведения занятий лекционного типа, оборудованные доской, столами, стульями.
2. Специальные помещения - учебные аудитории для проведения: занятий семинарского типа, групповых и индивидуальных консультаций, оборудованные доской, столами, стульями.
3. Специальные помещения - учебные аудитории для проведения лабораторных занятий, оборудованные доской, столами лабораторными, стульями, лабораторным оборудованием различной степени сложности:
4. Специальные помещения - учебные аудитории для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, оборудованные доской, столами, стульями.
5. Специальные помещения - учебные аудитории для организации и проведения самостоятельной работы студентов, оборудованные доской, компьютерами с возможностью подключения к сети «Интернет», столами, стульями.

Лист согласования рабочей программы дисциплины «Защита информации» на учебный год

Рабочая программа дисциплины «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)*
2020 – 2021	7.09.20
2021 – 2022	7.09.21
2022 – 2023	
2023 – 2024	

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)

Паспорт
фонда оценочных средств
по дисциплине «Защита информации »
(наименование дисциплины)

№ п/п	Раздел Дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Введение. Информационная безопасность: основные понятия и определения	ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	работа на практических: текущий контроль выполнения заданий; зачет
2	Анализ угроз информационной безопасности и методология построения систем защиты информации	ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет
3	Комплексный подход к обеспечению информационной безопасности	ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	работа на практических занятиях: текущий контроль выполнения заданий; зачет
4	Технологии обеспечения безопасности информации в автоматизированных системах	ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет

Описания элементов ФОС

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

1. Классификация информации по режиму использования. Общедоступная информация.
2. Классификация информации по режиму использования. Виды информации ограниченного доступа.
3. Классификация информации по режиму использования. Коммерческая тайна. Правила отнесения информации к коммерческой тайне.
4. Классификация информации по режиму использования. Правила отнесения информации к государственная тайна. Уровни секретности информации.
5. Понятие «информационной безопасности». Доктрина ИБ, угрозы в области информационной безопасности. Структура органов, ответственных за обеспечение ИБ.
6. Понятие «информационной безопасности». Составляющие информационной безопасности. Классификация методов защиты информации. Организации - регуляторы в области ИБ.
7. Нормативно- правовое регулирование в области ИБ. 149-ФЗ «Об информации ...»
8. Нормативно- правовое регулирование в области ИБ. Виды ответственности за нарушение режима ИБ. Уголовная ответственности за нарушение режима ИБ (статьи УК РФ).
9. Законодательство в области защиты персональных данных. Классификация информационных систем персональных данных. Требования по защите персональных данных
10. 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.

11. Угрозы ИБ. Каналы утечки информации.
12. Понятие модели угроз. Модели угроз для информационных систем персональных данных. (Примеры)
13. Классификация компьютерных вирусов по деструктивным возможностям.
14. Виды "вирусоподобных" программ. Поясните механизм функционирования "троянской программы", «логической бомбы», макровируса
15. Классификация криптографических систем. Назовите наиболее известные криптографические отечественные и зарубежные алгоритмы и дайте им краткую характеристику.
16. Матрица доступа принципы составления. Примеры
17. Анализ рисков информационной безопасности. Методики и программные продукты для оценки рисков
18. Принципы реализации симметричного метода шифрования
19. Принципы реализации асимметричного метода шифрования
20. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
21. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
22. Биометрические средства идентификации и аутентификации пользователей.
23. Аутентификация субъектов в распределенных системах. Метод одноразовых паролей, метод рукопожатия
24. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
25. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
26. Законодательный уровень применения цифровой подписи. Понятие и применение сертификата.

Критерии оценки:

Приведены в разделе 2

Наименование: работа на практических занятиях: текущий контроль выполнения заданий.

***Представление в ФОС*:** перечень заданий

Варианты заданий:

- Дайте определение термину "информационная безопасность"
- Проанализируйте основные положения ФЗ-149 "Об информации, информационных технологиях и защите информации"
- 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

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

2 Критерии оценки:

Уровень освоения компетенции							
	Компетенции	**Дескрипторы**	**Вид, форма оценочного мероприятия**	**Компетенция освоена***			
				отлично	**хорошо**	**удовлетворительно**	**неудовлетворительно**
	ПК-8 Способен обеспечивать информационную безопасность уровня баз данных.	З1. Знание политики безопасности РФ в области информационной безопасности З2. Знание основных угроз и каналов утечки информации; З3. Знание методов комплексного обеспечения информационной безопасности	Зачет	заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.	заслуживает обучающийся, обнаруживший полное знание учебного материала, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, знакомых с основной литературой, рекомендованной программой. Оценка выставляется обучающимся, допустившим погрешности в ответе на зачете и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.	выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине
		У1. Умение составлять содержание и план работы в профессиональной области с учетом требований информационной безопасности Н1. Владеет навыками применения методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы	Защита лабораторных работ	выставляется студенту, если задание выполнено в полном объёме с соблюдением необходимой последовательности. Студенты работают полностью самостоятельно: подбирают необходимые для выполнения предлагаемых работ в задании источники знаний, показывают необходимые для проведения практической работы теоретические знания, практические умения и навыки.	выставляется студенту, если задание выполнено в полном объёме и самостоятельно. Допускаются отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Студенты используют указанные преподавателем источники знаний, включая страницы атласа, таблицы из приложения к учебнику, страницы из справочной литературы по предмету. Задание показывает знание учащихся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Могут быть неточности и небрежность в оформлении результатов работы.	выставляется студенту, если задание на работу выполняется и оформляется студентами при помощи преподавателя или хорошо подготовленных и уже выполненных на «отлично» данную работу студентов. На выполнение задания затрачивается много времени (можно дать возможность доделать работу дома). Студенты показывают знания теоретического материала, но испытывают затруднение при решении конкретной задачи.	выставляется, если студенты показывают плохое знание теоретического материала и отсутствие умения применить знания к решению практической задачи. Руководство и помощь со стороны преподавателя и хорошо подготовленных студентов неэффективны по причине плохой подготовки студента..

		У1. Умение составлять содержание и план работы в профессиональной области с учетом требований информационной безопасности Н1. Владеет навыками применения методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы	Работа на практических занятиях: текущий контроль выполнения заданий	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие Способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению