**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

_____ И.А. Давыдов

25 июня 2018 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине: Защита информации
(наименование – полностью)

для направления: 09.03.01 «Информатика и вычислительная техника»
(шифр, наименование – полностью)

по профилю: Автоматизированные системы обработки информации и управления
(наименование – полностью)

форма обучения: очная
(очная, очно-заочная или заочная)

Общая трудоемкость дисциплины составляет: 5 зачетных единиц(ы)

| Вид учебной работы | Всего часов | Семестры | | | |
|---|---|---|---|---|---|
| | | 7 | | | |
| **Контактные занятия (всего)** | 74 | 74 | | | |
| В том числе: | - | - | - | - | - |
| Лекции | 30 | 30 | | | |
| Практические занятия (ПЗ) | 14 | 14 | | | |
| Семинары (С) | - | - | | | |
| Лабораторные работы (ЛР) | 30 | 30 | | | |
| **Самостоятельная работа (всего)** | 106 | 106 | | | |
| В том числе: | - | - | - | - | - |
| Курсовой проект (работа) | - | - | | | |
| Расчетно-графические работы | - | - | | | |
| Реферат | - | - | | | |
| *Другие виды самостоятельной работы* | 104 | 104 | | | |
| Вид промежуточной аттестации (зачет, экзамен) | Диф.зачет- 2 | Диф.зачет – 2ч. | | | |
| Общая трудоемкость час<br>зач. ед. | 180<br>5 | 180<br>5 | | | |

Кафедра «Организация вычислительных процессов и систем управления»

Составители Замятин Константин Игоревич, к.т.н., доцент,

Рабочая программа составлена на основании ФГОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника (уровень бакалавриата) №5 от 12.01.2016г. и утверждена на заседании кафедры

Протокол от « 19 » апреля 2018 г. № 04/18

Директор Воткинского филиала «ИжГТУ имени М.Т. Калашникова»

_____ И.А. Давыдов

« 19 » апреля 2018 г.

СОГЛАСОВАНО

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

_____ К.Б. Сентяков

« 19 » апреля 2018 г.

Количество часов рабочей программы соответствует количеству часов рабочего учебного плана направления 09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»

Ведущий специалист учебной части
ВФ ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»

_____ Соловьева Л.Н.

« 19 » апреля 2018 г.

Аннотация к дисциплине

| | | | | | |
|---|---|---|---|---|---|
| ***Название дисциплины*** | **Защита информации** | | | | |
| ***Номер*** | | ***Академический год*** | | ***семестр*** | **7** |
| ***кафедра*** | ***Программа*** | 09.03.01 «Информатика и вычислительная техника»<br>профиль «Автоматизированные системы обработки информации и управления» | | | |
| ***Составитель*** | Замятин Константин Игоревич, к.т.н., доцент, Стукалина Е.Ф., к.т.н., доцент | | | | |
| ***Цели и задачи дисциплины, основные темы*** | **Цели:** формирование способности принимать решения в профессиональной области с учетом требований информационной безопасности<br>**Задачи:** приобретение теоретических и практических знаний в организационно - правовых методах информационной безопасности, в криптографических и программно- аппаратных средствах защиты информации, а также в обеспечении информационной безопасности на различных стадиях жизненного цикла автоматизированной системы<br>**Знания**: политики безопасности РФ в области информационной безопасности; основных угроз и каналов утечки информации; методов комплексного обеспечения информационной безопасности<br>У**мения**: составлять содержание и план работы в профессиональной области с учетом требований информационной безопасности<br>**Навыки:** применения методов обеспечения информационной безопасности на различных стадиях жизненного цикла автоматизированной системы<br>**Лекции** (основные темы): Национальные интересы и безопасность России. Составляющие информационной безопасности. Основные принципы обеспечения информационной безопасности. Нормативно-правовое регулирование в области защиты информации. Угрозы информационной безопасности и каналы утечки информации. Методы разграничения доступа к информации. Криптографические методы защиты информации. Симметричные, ассиметричные шифры. Идентификация и аутентификация. Протокол Kerberos. Цифровая подпись.<br>**Лабораторные работы:** Виды информации ограниченного доступа; Макровирусы; Основы криптографии. Методы шифрования; Программно-аппаратные средства защиты данных; Цифровые сертификаты. | | | | |
| ***Основная литература*** | 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 | | | | |
| ***Технические средства*** | Учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации обучающихся, для самостоятельной работы студентов | | | | |
| ***Компетенции*** | ***Приобретаются студентами при освоении дисциплины***<br>ОПК-5 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br>ПК-2 Способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования | | | | |

| ***Зачетных единиц*** | ***5*** | ***Форма проведения занятий*** | ***Лекции*** | ***Практические занятия*** | ***Лабораторные работы*** | ***Самостоятельная работа*** |
|---|---|---|---|---|---|---|
| | | ***Всего часов*** | 30 | 30 | 30 | 90 |

| ***Виды контроля формы*** | ***Диф.зач /зач/ экз*** | ***КП/КР*** | ***Условие зачета дисципли-ны*** | Получение оценки 3,4,5 | ***Форма проведения самостоятельной работы*** | *Подготовка к практическим, лабораторным занятиям и зачету* |
|---|---|---|---|---|---|---|
| | Диф. зачет | - | | | | |

| | |
|---|---|
| ***Перечень дисциплин, знание которых необходимо для изучения данной дисциплины*** | Информатика, Программирование |

## 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 вариативной части Блока 1 «Дисциплины (модули) ООП».

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.

## 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 | Знания (№№ из 3.1) | Умения (№№ из 3.2) | Навыки (№№ из 3.3) |
|---|---|---|---|
| ОПК-5 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | 1,2,3 | 1 | 1 |
| ПК-2 Способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования | 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 | 7 | 1<br>2<br>3 | 2<br>2<br>2 | 2<br>2<br>2 | 2<br>2<br>2 | 10 | работа на практических и лабораторных занятиях; ответы на вопросы<br>Подготовка к зачету |
| 2 | Анализ угроз информационной безопасности и методология построения систем защиты информации | 7 | 4<br>5<br>6<br>7<br>8 | 2<br>2<br>2<br>2<br>2 | 2<br>2<br>2<br>2<br>2 | 2<br>2<br>2<br>2<br>2 | 40 | работа на практических и лабораторных занятиях; ответы на вопросы<br>Подготовка к зачету |
| 3 | Комплексный подход к обеспечению информационной безопасности | 7 | 9<br>10<br>11<br>12 | 2<br>2<br>2<br>2 | 2<br>2<br>2<br>2 | 2<br>2<br>2<br>2 | 20 | работа на практических и лабораторных занятиях; ответы на вопросы<br>Подготовка к зачету |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4 | Технологии обеспечения безопасности информации в автоматизированных системах | 7 | 13<br>14<br>15 | 2<br>2<br>2 | 2<br>2<br>2 | 2<br>2<br>2 | 18 | работа на практических и лабораторных занятиях; ответы на вопросы<br>Подготовка к зачету |
| | Зачет | | | | | | 2 | Вопросы к зачету |
| | Всего | | | 30 | 30 | 30 | 90 | |
| | В том числе контроль самостоятельной работы | | | | 2 | | | |

### 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.<br>2. Составляющие информационной безопасности. Основные принципы обеспечения информационной безопасности. Методы и инструменты обеспечения информационной безопасности<br>3. Нормативно-правовое регулирование в области защиты информации | 1,3 | 1 | 1 |
| 2 | 1. Угрозы информационной безопасности и каналы утечки информации<br>2. Классификация компьютерных вирусов<br>3. Стандарты информационной безопасности<br>4. Методы разграничения доступа к информации<br>5. Политика информационной безопасности.<br>6. Лицензирование, сертификация в области информационной безопасности<br>7. Анализ рисков информационной безопасности | 1,2,3 | 1 | 1 |
| 3 | 1. Организационно правовое обеспечение информационной безопасности.<br>2. Криптографические методы защиты информации. Симметричные, ассиметричные шифры.<br>3. Программно – технические методы и средства обеспечения ИБ | 1,3 | 1 | 1 |
| 4 | 1. Идентификация и аутентификация. Протокол Kerberos.<br>2. Функции хэширования.<br>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 | Трудоем-кость (час) |
|---|---|---|---|
| 1. | 1 | Анализ терминов и определений информационной безопасности | 2 |
| 2. | 1 | Национальные интересы РФ в области ИБ, приоритетные направления в области защиты информации. Органы, обеспечивающие национальную безопасность РФ | 2 |
| 3. | 1 | Виды информации. Правовое обеспечение защиты информации. Классификация информационных систем персональных данных | 2 |
| 4 | 2 | Угрозы ИБ. Понятие модели угроз. Модель злоумышленника. | 4 |
| 5 | 2 | Стандарты информационной безопасности. | 2 |
| 6 | 2 | Политика безопасности предприятия | 2 |
| | 2,3 | Составление матрицы доступа. Анализ и подбор сертифицированных средств защиты информации | 4 |
| 7 | 3 | Криптографические алгоритмы защиты информации. | 6 |
| 8 | 4 | Алгоритм цифровой подписи. Алгоритмы хэш-функций. Стандарты РФ на криптографические алгоритмы | 6 |
| | **Всего** | | **30** |

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

| № п/п | № раздела дисциплины | Наименование лабораторных работ | Трудоем-кость (час) |
|---|---|---|---|
| 1. | 1 | Виды информации ограниченного доступа. Классификация и требования нормативных документов к информационным системам персональных данных. | 6 |
| 2. | 2 | Макровирусы | 10 |
| 3. | 3 | Основы криптографии. Методы шифрования | 6 |
| 4. | 3,4 | Программно-аппаратные средства защиты данных | 6 |
| 5. | 4 | Цифровые сертификаты. Установка, настройка программного обеспечения криптопровайдеров. | 2 |
| | **Всего** | | **30** |

## 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 | 10 |
| **2.** | 2 | Модель нарушителя информационных систем | 10 |
| **3** | 2 | Классификация компьютерных вирусов и методов защиты информации | 10 |
| **4** | 2 | Системы обнаружения вторжений. Инциденты информационной безопасности. | 10 |

| | | | |
|---|---|---|---|
| **5** | 2 | Методики и программные продукты для оценки рисков | 10 |
| **6** | 3,4 | Криптографические алгоритмы защиты информации | 23 |
| **7** | 4 | Инфраструктура открытых ключей. Цифровые сертификаты | 15 |
| | | зачет | 2 |
| | **Всего** | | **90** |

**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 |
|---|---|---|
| 1 | 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(свободное ПО)
2. PGP (свободное ПО)

**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 с. — 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, экраном, проектором, 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, компьютерами с возможностью подключения к сети «Интернет», столами, стульями.
4. Специальные помещения - учебные аудитории для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, оборудованные доской, экраном, проектором, компьютерами с возможностью подключения к сети «Интернет», 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 утверждения рабочей программы дисциплины «Защита информации» на учебный год**

Рабочая программа дисциплины «Защита информации» утверждена на ведение учебного процесса в учебном году:

| ***Учебный год*** | ***«Согласовано»:*** *заведующий кафедрой, ответственной за РПД* *(подпись и дата)* |
|---|---|
| 2018- 2019 | |
| 2019- 2020 | |
| 2020- 2021 | |
| 2021 – 2022 | |
| 2022 - 2023 | |
| 2023 - 2024 | |
| 2024- 2025 | |

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»)

Кафедра Организация вычислительных процессов и систем управления
(наименование кафедры)

УТВЕРЖДЕН
на заседании кафедры
«__» _____2018 г., протокол №___
Директор филиала
_____ Давыдов И.А
(подпись)

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## ПО ДИСЦИПЛИНЕ

**«Защита информации»**
(наименование дисциплины)

**09.03.01 «Информатика и вычислительная техника»**
(шифр и наименование направления/специальности)

**Автоматизированные системы обработки информации и управления**
( наименование профиля/специализации/магистерской программы)

бакалавр
Квалификация (степень) выпускника

# 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 | ОПК-5 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 2 | Анализ угроз информационной безопасности и методология построения систем защиты информации | ОПК-5 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 3 | Комплексный подход к обеспечению информационной безопасности | ОПК-5, ПК-2 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 4 | Технологии обеспечения безопасности информации в автоматизированных системах | ОПК-5, ПК-2 | 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** |
| | ОПК-5 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br><br>ПК-2 Способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования | З1. Знание политики безопасности РФ в области информационной безопасности<br>З2. Знание основных угроз и каналов утечки информации;<br>З3. Знание методов комплексного обеспечения информационной безопасности | Диф. 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<br><br>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<br><br>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.<br>Продемонстрирован высокий уровень владения материалом.<br>Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий. | Правильно выполнена большая часть заданий.<br>Присутствуют незначительные ошибки.<br>Продемонстрирован хороший уровень владения материалом.<br>Проявлены средние способности применять знания и умения к выполнению конкретных заданий | Задания выполнены более чем наполовину.<br>Присутствуют серьёзные ошибки.<br>Продемонстрирован удовлетворительный уровень владения материалом.<br>Проявлены низкие Способности применять знания и умения к выполнению конкретных заданий. | Задания выполнены менее чем наполовину.<br>Продемонстрирован неудовлетворительный уровень владения материалом.<br>Проявлены недостаточные способности применять знания и умения к выполнению |
| | | | | | | | |

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»)

Кафедра Организация вычислительных процессов и систем управления
(наименование кафедры)

УТВЕРЖДЕН
на заседании кафедры
«19» апр. 2018 г., протокол №04/18
Директор филиала
_____ Давыдов И.А
(подпись)

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## ПО ДИСЦИПЛИНЕ

**«Защита информации»**
(наименование дисциплины)

**09.03.01 «Информатика и вычислительная техника»**
(шифр и наименование направления/специальности)

**Автоматизированные системы обработки информации и управления**
( наименование профиля/специализации/магистерской программы)

бакалавр
Квалификация (степень) выпускника

# 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 | ОПК-5 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 2 | Анализ угроз информационной безопасности и методология построения систем защиты информации | ОПК-5 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 3 | Комплексный подход к обеспечению информационной безопасности | ОПК-5, ПК-2 | работа на практических и лабораторных занятиях: текущий контроль выполнения заданий; зачет |
| 4 | Технологии обеспечения безопасности информации в автоматизированных системах | ОПК-5, ПК-2 | 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** |
| | ОПК-5 Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности<br><br>ПК-2 Способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования | З1. Знание политики безопасности РФ в области информационной безопасности<br>З2. Знание основных угроз и каналов утечки информации;<br>З3. Знание методов комплексного обеспечения информационной безопасности | Диф. 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<br><br>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<br><br>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.<br>Продемонстрирован высокий уровень владения материалом.<br>Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий. | Правильно выполнена большая часть заданий.<br>Присутствуют незначительные ошибки.<br>Продемонстрирован хороший уровень владения материалом.<br>Проявлены средние способности применять знания и умения к выполнению конкретных заданий | Задания выполнены более чем наполовину.<br>Присутствуют серьёзные ошибки.<br>Продемонстрирован удовлетворительный уровень владения материалом.<br>Проявлены низкие Способности применять знания и умения к выполнению конкретных заданий. | Задания выполнены менее чем наполовину.<br>Продемонстрирован неудовлетворительный уровень владения материалом.<br>Проявлены недостаточные способности применять знания и умения к выполнению |