МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**

Заведующий кафедрой
*информационных систем*
*доцент Борисов Д.Н.,*
*подпись, расшифровка подписи*
10.04.2024.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ФТД.01 Защита персональных данных
*Код и наименование дисциплины в соответствии с учебным планом*

**1. Код и наименование направления подготовки/специальности:**
*10.05.01 Компьютерная безопасность*

**2. Профиль подготовки/специализация:** *Анализ безопасности компьютерных систем*

**3. Квалификация выпускника:** *Специалист*

**4. Форма обучения:** *Очная*

**5. Кафедра, отвечающая за реализацию дисциплины:** *информационных систем*

**6. Составители программы:** Борисова Алла Александровна, к.и.н., доцент

_____
_____

**7. Рекомендована:** _НМС ФКН, протокол № 5 от 05.03.2024.
*(наименование рекомендующей структуры, дата, номер протокола,*
_____
*отметки о продлении вносятся вручную)*

**8. Учебный год:**___ 2028-2029_____ **Семестр(ы):** ___9__

**9.Цели и задачи учебной дисциплины**

**Цели и задачи учебной дисциплины**

*Целями освоения учебной дисциплины являются:*

- *понимание основных аспектов защиты персональных данных;*
- *изучение предъявляемых требований и мер, необходимых для обеспечения защиты персональных данных;*

*Задачи учебной дисциплины:*

- *приобретение практических навыков проектирования систем защиты персональных данных согласно требованиям законодательства Российской Федерации.*

**10. Место учебной дисциплины в структуре ООП** дисциплина относится к дисциплинам, формируемой участниками образовательных отношений. Факультативы. Требуется предварительное знание информатики, введение в программирование.

**11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:**

| Код и название компетенции | Код и название индикатора компетенции | Знания, умения, навыки |
|---|---|---|
| ПК-3 Способен проводить анализ безопасности программных средств в компьютерных системах | ПК-3.2 знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования | Знать: современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования для защиты персональных данных, контроля целостности данных. |
| ПК-3 Способен проводить анализ безопасности программных средств в компьютерных системах | ПК-3.4 умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента | Уметь: анализировать возможности использования современных технологий защиты данных и объектов электронного контента в области защиты персональных данных |

**12. Объем дисциплины в зачетных единицах/час** — *2 / 72*

**Форма промежуточной аттестации** зачет

**13. Трудоемкость по видам учебной работы**

| Вид учебной работы | № сем. 9 | Всего |
|---|---|---|
| Аудиторные занятия | 32 | 32 |
| лекции | 16 | 16 |
| практические | 16 | 16 |
| лабораторные | 0 | 0 |
| Самостоятельная работа | 40 | 40 |
| Форма промежуточной аттестации *(зачет – час..)* | зачет | |
| Итого: | 72 | 72 |

**13.1. Содержание дисциплины**

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины | Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК * |
|---|---|---|---|
| **1. Лекции** | | | |
| 1.1 | Основы защиты информационных систем персональных данных | Основные характеристики информационной системы персональных данных (ИСПД). Обработка персональных данных (ПД). | |
| 1.2 | Законодательство в сфере защиты ПД | ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты ПД. Категории ПД. | |
| 1.3 | Требования по обеспечению безопасности ПД | Набор требований, определяющих выбор мер защиты ПД в ИСПД. | |
| 1.4 | Основные этапы разработки систем защиты персональных данных (СЗПД) | Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты ПД, реализация мер защиты, проверка выполнения требований. | |
| 1.5 | Документационное обеспечение СЗПД | Виды документов, разрабатываемых при создании СЗПД | |
| 1.6 | Моделирование угроз безопасности ПД | Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021. Определение уровня защищённости ИСПД. | |
| 1.7 | Проектирование СЗПД часть 1 | Проектирование СЗПД для определения перечня мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований. | |
| 1.8 | Проектирование СЗПД часть 2 | Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД | |
| 1.9 | Испытания и ввод в действие СЗПД | Определение состава и содержания проверок реализации мер защиты ПД, проведение проверок. Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие СЗПД. | |
| **2. Практические занятия** | | | |
| 2.1 | Моделирование ИСПД | Разработка практической модели ИСПД, определение бизнес-процессов, требующих обработки ПД, и видов обработки ПД. | |
| 2.2 | Определение требований к СЗПД | Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты ПД. | |
| 2.3 | Моделирование угроз безопасности ПД, определение уровня защищённости ИСПД | Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021. Определение уровня защищённости ИСПД. | |
| 2.4 | Формирование документа на разработку СЗПД | Формирование документа на разработку СЗПД, определяющего перечень мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований. | |
| 2.5 | Формирование документов, определяющих функции средств защиты информации | Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД. | |
| 2.6 | Формирование эксплуатационной документации | Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек. | |
| 2.7 | Формирование | Формирование программы и методики испытаний, | |

| | | | |
|---|---|---|---|
| | документации по испытаниям и вводу в действие СЗПД | документа оценки эффективности принятых мер, ввод в действие СЗПД | |

### 13.2. Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование темы (раздела) дисциплины | Виды занятий (количество часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Практические | Лабораторные | Самостоятельная работа | Всего |
| 1 | Основы защиты информационных систем персональных данных | 1 | 1 | | 4 | 6 |
| 2 | Законодательство в сфере защиты ПД | 1 | 1 | | 4 | 6 |
| 3 | Требования по обеспечению безопасности ПД | 2 | 1 | | 4 | 7 |
| 4 | Основные этапы разработки систем защиты персональных данных (СЗПД) | 2 | 2 | | 4 | 8 |
| 5 | Документационное обеспечение СЗПД | 2 | 1 | | 4 | 7 |
| 6 | Моделирование угроз безопасности ПД | 2 | 1 | | 4 | 7 |
| 7 | Проектирование СЗПД часть 1 | 2 | 3 | | 6 | 11 |
| 8 | Проектирование СЗПД часть 2 | 2 | 3 | | 6 | 11 |
| 9 | Испытания и ввод в действие СЗПД | 2 | 3 | | 4 | 9 |
| | Итого | 16 | 16 | | 40 | 72 |

## 14. Методические указания для обучающихся по освоению дисциплины

Студентам читать рекомендованную литературу, во время проверки выполнения лабораторных работ, преподавателю рекомендуется проводить теоретический опрос с целью определения степени усвоения материала.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

| № п/п | Источник |
|---|---|
| *1* | *Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. — Уфа : БашГУ, 2020. — 120 с. — ISBN 978-5-7477-5228-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179914* |
| *2* | *Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175506* |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| *1* | *Гусев, А. Ю. Судебная практика о применении законодательства, регулирующего вопросы защиты персональных данных : учебное пособие / А. Ю. Гусев. — Москва : Проспект, 2019. — 63 с. — ISBN 978-5-392-29690-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151026* |
| *2* | *Дупан (Гутникова), А. С. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / А. С. Дупан (Гутникова), А. Б. Жулин, А. К. Жарова ; под редакцией* |

| | |
|---|---|
| | *Дупан (Гутниковой) А.С.. — Москва : Высшая школа экономики, 2016. — 344 с. — ISBN 978-5-7598-1386-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100135* |
| *3* | *Ильин, О. Ю. Актуальные вопросы российского права: защита персональных данных, антикоррупционное законодательство, правовой статус личности, противодействие терроризму и экстремистской деятельности : учебное пособие / О. Ю. Ильин. — Тверь : ТвГТУ, 2020. — 104 с. — ISBN 978-5-7995-1114-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171323* |

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

| № п/п | Ресурс |
|---|---|
| 1. 6 | www.lib.vsu.ru – *ЗНБ ВГУ* |

## 16. Перечень учебно-методического обеспечения для самостоятельной работы

| № п/п | Источник |
|---|---|
| *1* | *Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744* |
| *2* | *Организация защиты персональных данных : учебное пособие / составители А. М. Макаров [и др.]. — Ставрополь : СКФУ, 2015. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155243* |

## 17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

---

## 18. Материально-техническое обеспечение дисциплины:

1) лекционная аудитория, оснащенная мультимедиа проектором;
2) класс для проведения практических занятий;

---

## 19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

| № п/п | Раздел дисциплины (модуля) | Код компетенции | Код индикатора | Оценочные средства для текущей аттестации |
|---|---|---|---|---|
| 1 | Моделирование ИСПД и определение требований к СЗПД | ПК-3 | ПК-3.2, ПК-3.4. | Контрольная работа 1 |
| 2 | Моделирование угроз безопасности ПД, определение уровня защищённости ИСПД | ПК-3 | ПК-3.2, ПК-3.4 | Контрольная работа 2 |
| 3 | Проектирование, испытания и ввод в действие СЗПД | ПК-3 | ПК-3.2, ПК-3.4 | Контрольная работа 3 |

Промежуточная аттестация

Форма контроля – зачет

## 20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

### 20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях;

Контрольная работа по теоретической части курса;

Практические работы.

| № п/п | Наименование оценочного средства | Представление оценочного средства в фонде | Критерии оценки |
|---|---|---|---|
| 1 | Устный опрос на практических занятиях | Вопросы по темам/разделам дисциплины | Правильный ответ – зачтено, неправильный или принципиально неточный ответ<br>- не зачтено |
| 2 | Контрольная работа по разделам дисциплины | Теоретические вопросы по темам/разделам дисциплины | Шкала оценивания соответствует приведенной ниже |
| 3 | Практическая работа | Содержит 9 практических заданий, предусматривающих разработку, тестирование и эксплуатацию различных криптографических и стеганографических алгоритмов. | При успешном выполнении работы ставится оценка зачтено, в противном случае ставится оценка не зачтено |

Пример задания для выполнения практической работы

Контрольная работа 1

Вариант 1

1) Основные характеристики информационной системы персональных данных.

2) Набор требований, определяющих выбор мер защиты персональных данных и в информационной системы персональных данных.

3) Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты персональных данных.

Вариант 2

1) Обработка персональных данных.

2) Набор требований, определяющих выбор мер защиты персональных данных и в информационной системы персональных данных.

3) Разработка практической модели информационной системы персональных данных, определение бизнес-процессов, требующих обработки персональных данных, и видов обработки персональных данных.

Вариант 3

1) Основные характеристики информационной системы персональных данных.

2) ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты персональных данных. Категории персональных данных.

3) Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты персональных данных.

Контрольная работа 2

Вариант 1

1) Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты персональных данных, реализация мер защиты, проверка выполнения требований.

2) Определение актуальных нарушителей и угроз безопасности персональных данных на основе Методики ФСТЭК 2021.

Вариант 2

1) Виды документов, разрабатываемых при создании систем защиты персональных данных

2) Определение уровня защищённости информационной системы персональных данных.

Вариант 3

1) Определение актуальных нарушителей и угроз безопасности персональных данных на основе Методики ФСТЭК 2021.

2) Формирование документа на разработку систем защиты персональных данных, определяющего перечень мер, необходимых для обеспечения безопасности персональных данных на основе предъявляемых требований.

Контрольная работа 3

Вариант 1

1) Проектирование систем защиты персональных данных для определения перечня мер, необходимых для обеспечения безопасности персональных данных на основе предъявляемых требований.

2) Определение состава и содержания проверок реализации мер защиты персональных данных, проведение проверок.

3) Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие систем защиты персональных данных

Вариант 2

1) Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности персональных данных

2) Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие систем защиты персональных данных.

3) Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек

Вариант 3

1) Проектирование систем защиты персональных данных для определения перечня мер.

2) Проектирование систем защиты персональных данных выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности персональных данных.

3) Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие систем защиты персональных данных

Приведенные ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний:

ПК-3

Задания закрытого типа

1. В каком документе указывается цель и задачи обработки персональных данных?

а) базовая модель угроз

б) инструкция по обеспечению безопасности персональных данных

в) частная модель угроз

г) положение по обеспечению безопасности персональных данных

2. На каком этапе создания системы защиты персональных данных определяется состав персональных данных и необходимость их обработки?

а) эксплуатация

б) стадия проектирования

в) предпроектная стадия

г) ввод в действие

3. На каком этапе построения системы защиты персональных данных происходит выявление технических каналов утечки информации?

а) оценка обстановки

б) разработка замысла защиты

в) решение вопросов управления защитой

г) реализация замысла защиты

4. Какому принципу обеспечения безопасности персональных данных соответствует то, что системы обеспечения безопасности персональных данных должны строиться с учетом возможного изменения конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации?

а) принцип оптимальной и разумной разнородности

б) принцип преемственности и совершенствования

в) принцип превентивности

г) принцип адаптивности

5. Какие органы сертификации средств защиты информации работают в области обеспечения безопасности персональных данных? (Выберите несколько вариантов ответа)

а) Ростехнадзор

б) ФСТЭК

в) Роскомнадзор

г) ФСБ

6. Какие категории персональных данных выделяет ФЗ “О персональных данных”? (Выберите несколько вариантов ответов.)

а) биометрические

б) специальные

в) общедоступные

г) личные

д) физиологические

7. К какой категории персональных данных можно отнести адресную книгу?

а) общедоступные

б) дополнительные

в) биометрические

г) специальные

8. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на:

а) администратора безопасности информационной системы персональных данных

б) оператора персональных данных

в) доверенное лицо

г) субъекта персональных данных

9. Защищаемая информация – это

а) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

б) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации;

в) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов;

г) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации».

10. Доступ к информации – это

а) Возможность получения информации и ее использования;

б) Возможность использования информации;

в) Возможность доступа к информации;

г) Возможность доступа к информации, но не ее использования.

## Задания открытого типа

1. Имитация сайтов финансовых учреждений злоумышленником с целью похищения информации называется:_____

2. Как называется похищение реквизитов банковских карт злоумышленником?_____

3. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?_____

4. Как называется лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам?_____

5. Сколько регуляторов в области обеспечения безопасности персональных данных?_____

6. Основополагающим федеральным законом в области обеспечения безопасности персональных данных является:_____

7. Какой орган является регулятором в части, касающейся соблюдения требований по организации и обеспечению функционирования криптографических средств в случае их использования для обеспечения безопасности персональных данных?_____(аббревиатура)

8. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?_____

9. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?_____

10. Как называется попытка реализации угрозы?_____

Задания с развернутым ответом

1. Организация «Ромашка» передает данные о работниках для оценки их деловых качеств третьим лицам – специализированной организации, производящей оценку персонала. В частности, передаются специально разработанные анкеты, содержащие фамилию, имя, отчество, год, месяц, дату и место рождения, адрес работника. Согласия на передачу персональных данных у работника не получено. Каким образом возможно передать сведения третьему лицу, не нарушая законодательство о защите персональных данных?

Решение задачи должно быть обосновано правовыми нормами.

## 20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня практических работ, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Соотношение показателей, критериев и шкалы оценивания результатов обучения представлено в следующей таблице.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

| Критерии оценивания компетенций | Уровень сформированности компетенций | Шкала оценок |
|---|---|---|
| Знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, выполнение заданий, предусмотренных программой, знакомство с основной литературой, рекомендованной программой. Присутствуют погрешности в ответе на зачете и при выполнении контрольных заданий. | | *Зачет* |
| Имеются пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в выполнении предусмотренных программой заданий, наличие которых препятствует дальнейшему обучению студента. | | *Не зачет* |

КИМ формируется из трех теоретических вопросов и одной практической задачи.

Перечень вопросов к зачету:

1. Основные характеристики информационной системы персональных данных (ИСПД). Обработка персональных данных (ПД).
2. ФЗ-152, Постановление Правительства РФ №1119, основные документ ФСТЭК и ФСБ в сфере защиты ПД. Категории ПД.
3. Набор требований, определяющих выбор мер защиты ПД в ИСПД.
4. Основные этапы разработки систем защиты персональных данных (СЗПД): обследование, моделирование угроз, определение требований и выбор мер защиты ПД, реализация мер защиты, проверка выполнения требований.
5. Виды документов, разрабатываемых при создании СЗПД
6. Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021.
7. Определение уровня защищённости ИСПД.
8. Проектирование СЗПД для определения перечня мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.
9. Выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД
10. Определение состава и содержания проверок реализации мер защиты ПД, проведение проверок.
11. Подтверждение соответствия принятых мер требованиям по обеспечению безопасности ПД, ввод в действие СЗПД.
12. Разработка практической модели ИСПД, определение бизнес-процессов, требующих обработки ПД, и видов обработки ПД.
13. Определение набора требований на основе Постановления Правительства РФ №1119, основных документов ФСТЭК и ФСБ в сфере защиты ПД.
14. Определение актуальных нарушителей и угроз безопасности ПД на основе Методики ФСТЭК 2021.
15. Определение уровня защищённости ИСПД.
16. Формирование документа на разработку СЗПД, определяющего перечень мер, необходимых для обеспечения безопасности ПД на основе предъявляемых требований.
17. Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению безопасности ПД.
18. Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек.
19. Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие СЗПД.