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

УТВЕРЖДАЮ

Заведующий кафедрой
информационных систем
доцент Борисов Д.Н.,
03.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ФТД.В.01 Методы защиты информационных систем
Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализация: *Анализ и синтез информационных систем, Информационные технологии в менеджменте, Системы прикладного искусственного интеллекта*

3. Квалификация выпускника: *Магистр*

4. Форма обучения: *Очная*

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

6. Составители программы: Борисов Дмитрий Николаевич, к.т.н., доцент,

(ФИО, ученая степень, ученое звание)

_____

_____

7. Рекомендована: _НМС ФКН, протокол № 7 от 03.05.2023.
(наименование рекомендующей структуры, дата, номер протокола,

_____
отметки о продлении вносятся вручную)

8. Учебный год:___ 2023-2024_____ **Семестр(ы):** ___1__

9.Цели и задачи учебной дисциплины
Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- *понимание основных аспектов и методов защиты информационных систем;*
- *изучение принципов работы компонентов защиты информационных систем;*
- *изучение предъявляемых требований и мер, необходимых для обеспечения защиты информационных систем;*

Задачи учебной дисциплины:

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

10. Место учебной дисциплины в структуре ООП дисциплина относится к дисциплинам, формируемым 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
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	Знать: основные стадии разработки, принцип декомпозиции задач, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности данных.
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.2 Знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	Знать: алгоритмы построения систем защиты информации в информационных системах. Уметь: классифицировать угрозы безопасности, определять особенности защищаемых информационных систем
ОПК-3 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ОПК-3.1 Знает принципы, методы и средства анализа и структурирования профессиональной информации	Знать: принципы работы основных средств защиты информации, протоколы, интерфейсы и форматы обмена данными

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

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	№ сем. 1	Всего
Аудиторные занятия	36	36
лекции	18	18
практические	0	0
лабораторные	18	18
Самостоятельная работа	36	36
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	Основные характеристики информационной системы (ИС). Виды защищаемой информации в ИС.	
1.2	Законодательство в сфере защиты ИС	149-ФЗ, 187-ФЗ, 98-ФЗ, основные документы ФСТЭК и ФСБ в сфере защиты ИС.	
1.3	Требования по обеспечению безопасности ИС	Набор требований, определяющих выбор мер защиты ИС. Обоснование архитектуры и используемых технологий в ИС	
1.4	Идентификация и аутентификация, управление доступом	Идентификация. Аутентификация и управление доступом в ИС. Модели управления доступом.	
1.5	Защита сети	МЭ, VPN/СКЗИ, прокси, IDS, IPS.	
1.6	Антивирусная защита	Антивирусная защита рабочих станций, серверов, сервисов.	
1.7	Превентивные меры защиты	Сканирование на наличие уязвимостей. Противодействие разведке. Контроль и установка обновлений.	
1.8	Контроль действий и регистрация событий ИБ	Контроль действий пользователей и администраторов. События безопасности. Регистрация событий безопасности.	
1.9	Защита виртуальных сред, эшелонирование защиты	Защита виртуальных сред. Резервное копирование. Эшелонирование защиты.	
2. Лабораторные занятия			
2.1	Настройка идентификации и аутентификации	Настройка идентификации и аутентификации на операционных системах АРМ и серверов, сетевого оборудования.	
2.2	Управление доступом ч. 1	Управление доступом в операционных системах на базе Linuxи Windows.	
2.3	Управление доступом ч. 2	Управление доступом в ОС и ПО сетевого оборудования и средств защиты.	
2.4	Защита сети ч. 1	Настройка межсетевого экрана на базе ACL, настройка защищённого VPN-соединения клиент-сервер.	

2.5	Защита сети ч. 2	Установка и базовая настройка Suricata.	
2.6	Антивирусная защита	KES, KSM.	
2.7	Превентивные меры защиты	Сканирование сетей. Анализ сетевого трафика.	
2.8	Превентивные меры защиты ч. 2	Знакомство с Honeypot.	
2.9	Регистрация событий ИБ	Знакомство с системой мониторинга Zabbix.	

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	2		2	4	8
2	Законодательство в сфере защиты ИС	2		2	4	8
3	Требования по обеспечению безопасности ИС	2		2	4	8
4	Идентификация и аутентификация, управление доступом	2		2	4	8
5	Защита сети	2		2	4	8
6	Антивирусная защита	2		2	4	8
7	Превентивные меры защиты	2		2	4	8
8	Контроль действий и регистрация событий ИБ	2		2	4	8
9	Защита виртуальных сред, эшелонирование защиты	2		2	4	8
	Итого	18		18	36	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	*Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279*
2	*Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/326153*
3	*Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103200*
4	*Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва : МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701*

б) дополнительная литература:

№ п/п	Источник

1	*Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401*
2	*Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522*
3	*Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844*
46	*Буранова, М. А. Комплексная система защиты информации : учебное пособие / М. А. Буранова, Н. В. Киреева. — Самара : ПГУТИ, 2019. — 145 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223181*

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

№ п/п	Ресурс
9	www.lib.vsu.ru – *ЗНБ ВГУ*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	*Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159977*
2	*Комплексные системы защиты информации на предприятиях : учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома : КГУ им. Н.А. Некрасова, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/201884*
3	*Нестандартные методы защиты информации : учебное пособие / составители В. П. Пашинцев, А. В. Ляхов. — Ставрополь : СКФУ, 2016. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155239*

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	Требования по обеспечению безопасности ИС	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	Контрольная работа 1
2	Превентивные меры защиты	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	Контрольная работа 2

№ п/п	Раздел дисциплины (модуля)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
3	Защита виртуальных сред, эшелонирование защиты	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	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 лекционных занятиях;

Контрольная работа по теоретической части курса;

Лабораторные 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 - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной ниже
3	Лабораторная работа	Содержит 9 лабораторных заданий, предусматривающих настройку и эксплуатацию различных средств защиты информации.	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.

Пример задания для выполнения практической работы

Контрольная работа 1

Вариант 1

1) Определение характеристик информационной системы;

2) Набор требований, определяющих выбор мер защиты ИС;

3) Обоснование архитектуры и используемых технологий в ИС;

Примеры вопросов из теста:

Тестовый вопрос: Какой документ ФСТЭК определяет требования к защите информации в АСУ ТП

Варианты ответа:

1) Приказ ФСТЭК №21

2) Приказ ФСТЭК №31

3) Приказ ФСТЭК №17

Тестовый вопрос: Что является основным документом, регламентирующим использование средств криптографической защиты информации

Варианты ответа:

1) ФЗ-187

2) ФЗ-149

3) Приказ ФСБ №378

4) Приказ ФСТЭК №31

Контрольная работа 2

Вариант 1

1. Дать определение аутентификации. Привести примеры.

2. Дать определение идентификации в информационных системах

3. Дать определение авторизации пользователя

4. Дать определение пароля

Контрольная работа 3

Вариант 1

1. Системой криптографической защиты информации является:

а) BFox Pro

б) CAudit Pro

в) Крипто Про

2. Какие вирусы активизируются в самом начале работы с операционной системой:

а) загрузочные вирусы

б) троянцы

в) черви

3. Stuxnet — это:

а) троянская программа

б) макровирус

в) промышленный вирус

4. Таргетированная атака — это:

а) атака на сетевое оборудование

б) атака на компьютерную систему крупного предприятия

в) атака на конкретный компьютер пользователя

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

ОПК-2

Задания закрытого типа

1. Под информационной безопасностью понимается:

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

в) нет верного ответа

2. Защита информации:

а) небольшая программа для выполнения определенной задачи

б) комплекс мероприятий, направленных на обеспечение информационной безопасности

в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

3. Информационная безопасность зависит от:

а) компьютеров, поддерживающей инфраструктуры

б) пользователей

в) информации

4. Конфиденциальностью называется:

а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

б) описание процедур

в) защита от несанкционированного доступа к информации

5. Для чего создаются информационные системы:

а) получения определенных информационных услуг

б) обработки информации

в) оба варианта верны

6. Кто является основным ответственным за определение уровня классификации информации:

а) руководитель среднего звена

б) владелец

в) высшее руководство

7. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:

а) хакеры

б) контрагенты

в) сотрудники

8. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:

а) снизить уровень классификации этой информации

б) улучшить контроль за безопасностью этой информации

в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

9. Что самое главное должно продумать руководство при классификации данных:

а) управление доступом, которое должно защищать данные

б) оценить уровень риска и отменить контрмеры

в) необходимый уровень доступности, целостности и конфиденциальности

10. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:

а) владельцы данных

б) руководство

в) администраторы

Задания открытого типа

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

2. Как называется попытка реализации угрозы?_____

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

4. Если злоумышленник внедрил в компьютер вредоносную программу и получил доступ к личной информации пользователя, какое свойство информации было нарушено?_____

5. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?_____

6. Анна послала письмо Степану. Злоумышленник уничтожил письмо Анны, подсунул свое и отправил Степану от имени Анны. Какое свойство информации было нарушено?_____

7. Анна послала письмо Степану. Злоумышленник прочитал письмо Анны, подсунул вместо него свое и отправил Степану от имени Анны. Какое свойство(а) информации было(и) нарушено?_____, _____

8. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?_____

9. Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?_____

10. Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу?_____

Задания с развернутым ответом

1. Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте восемь первых букв из своих данных: Фамилии, Имени, Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые четыре буквы.

ОПК-3

Задания закрытого типа

1. Процедурой называется:

а) пошаговая инструкция по выполнению задачи

б) обязательные действия

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

2. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:

а) проведение тренингов по безопасности для всех сотрудников

б) поддержка высшего руководства

в) эффективные защитные меры и методы их внедрения

3. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

а) когда риски не могут быть приняты во внимание по политическим соображениям

б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски

в) когда стоимость контрмер превышает ценность актива и потенциальные потери

4. Что такое политика безопасности:

а) детализированные документы по обработке инцидентов безопасности

б) широкие, высокоуровневые заявления руководства

в) общие руководящие требования по достижению определенного уровня безопасности

5. Какая из приведенных техник является самой важной при выборе конкретных защитных мер:

а) анализ рисков

б) результаты ALE

в) анализ затрат / выгоды

6. Что лучше всего описывает цель расчета ALE:

а) количественно оценить уровень безопасности среды

б) оценить потенциальные потери от угрозы в год

в) количественно оценить уровень безопасности среды

7. Тактическое планирование:

а) среднесрочное планирование

б) ежедневное планирование

в) долгосрочное планирование

8. Эффективная программа безопасности требует сбалансированного применения:

а) контрмер и защитных механизмов

б) процедур безопасности и шифрования

в) технических и нетехнических методов

9. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) уровень доверия, обеспечиваемый механизмом безопасности

б) внедрение управления механизмами безопасности

в) классификацию данных после внедрения механизмов безопасности

10. Что из перечисленного не является целью проведения анализа рисков:

а) выявление рисков

б) делегирование полномочий +

в) количественная оценка воздействия потенциальных угроз

Задания открытого типа

1. Какой документ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?_____

2. Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?_____

3. Наукой, изучающей математические методы защиты информации путем ее преобразования, является: _____

4. Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем

5. По документам ГТК самый высокий класс защищенности СВТ от НСД к информации: _____(ответ цифрой)

6. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это _____

7. При избирательной политике безопасности в матрице доступа объекту системы соответствует _____.

8. При избирательной политике безопасности в матрице доступа субъекту системы соответствует: _____

9. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это: _____.

10. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется: _____

Задания с развернутым ответом

1. Вычислите (с подробным пояснением расчетов) децильный коэффициент, если 10 % от совокупного дохода наиболее богатого населения 3 млн долларов, а 10 % наименее обеспеченного – 200000 долларов?

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 экзамене и при выполнении экзаменационных 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 (ИС). Виды защищаемой информации в ИС.
2. 149-ФЗ, 187-ФЗ, 98-ФЗ, основные документы ФСТЭК и ФСБ в сфере защиты ИС.
3. Набор требований, определяющих выбор мер защиты ИС. Обоснование и регламентация используемых технологий в ИС.

4. Идентификация. Аутентификация и управление доступом в ИС.
5. Модели управления доступом.
6. Межсетевые экраны, VPN, прокси-серверы.
7. Системы обнаружения и предотвращения вторжений.
8. Антивирусная защита рабочих станций, серверов, сервисов.
9. Сканирование на наличие уязвимостей. Противодействие разведке.
10. Контроль и установка обновлений.
11. Контроль действий пользователей и администраторов.
12. События безопасности. Регистрация событий безопасности.
13. Защита виртуальных сред.
14. Резервное копирование.
15. Эшелонирование защиты.
16. Формирование документа, определяющего перечень мер, необходимых для обеспечения безопасности информации на основе предъявляемых требований.
17. Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению защиты информации.
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 системы защиты информации.