

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

25.01.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.25 Основы информационной безопасности

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность)	10.05.03 Информационная безопасность автоматизированных систем
Квалификация выпускника	Специалист (бакалавр/магистр/специалист)
Специализация	Безопасность автоматизированных систем критически важных объектов

Курс	3
Семестр	5

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	18	часов
Лабораторные работы	36	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	54	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	54	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	5	семестр
Зачет	-	семестр
БРК, ДЗ	-	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

заведующий кафедрой с ученой степенью доктора наук и ученым званием "профессор"	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)
старший преподаватель	ИБ	СОГЛАСОВАНО	В.И. Смирнов
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

	(наименование кафедры)		
25.01.2023	протокол №	10/1	
(дата)			
Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина	
		(И.О. Фамилия)	

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 06.03.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 знает сущность и понятие информации, информационной безопасности и характеристику ее составляющих	знания: знает сущность и понятие информации, информационной безопасности и характеристику ее составляющих умения: навыки:
	ОПК-1.2 умеет классифицировать и оценивать угрозы информационной безопасности.	знания: умения: умеет классифицировать и оценивать угрозы информационной безопасности навыки:
	ОПК-1.3 Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем	знания: знает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем умения: умеет моделировать автоматизированные системы и подсистемы безопасности автоматизированных систем навыки: исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем
2. ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированной	ОПК-6.1 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	знания: знает основные угрозы безопасности информации и модели нарушителя объекта информатизации умения: навыки:
	ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	знания: умения: умеет разрабатывать модели угроз и модели нарушителя объекта информатизации навыки:

нных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.3 Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	знания: знает меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем умения: умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем навыки: определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем
--	---	---

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Информационные технологии (ОПК-1)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Теория информации (ОПК-1), Теоретические основы компьютерной безопасности (ОПК-6); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-1), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-6)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия, процедуры самообучения

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция, лекция с элементами мозгового штурма

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Государственная информационная политика.	36	ОПК-1

Информационная безопасность и угрозы информационной безопасности. Общие принципы защиты информации		
Лекция. Обеспечение национальной безопасности РФ. Государственная информационная политика (технологический и содержательный аспекты)	2	
Лекция. Доктрина информационной безопасности. Государственные органы, связанные с обеспечением ИБ. Цели и задачи в области ИБ	2	
Лекция. Информационная война. Информационное оружие, его особенности и классификация. Классификация средств защиты и нападения	2	
Лабораторная работа. Лабораторная работа №1. Использование социальных сервисов для представления данных по информационной безопасности	6	
Лабораторная работа. Лабораторная работа №2. Информационные ресурсы, продукты и услуги. Правовые аспекты информационной деятельности	6	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций. Подготовка к лабораторным работам. Задания для самостоятельной работы.	18	
Безопасность (защищенность) информационных систем. Вредоносное программное обеспечение	36	ОПК-1, ОПК-6
Лекция. Понятие угрозы ИБ. Источники угроз, уязвимости ИС, атаки и последствия реализации угроз. Каналы утечки информации. Классификации угроз ИБ	2	
Лекция. Методы нарушения конфиденциальности, целостности и доступности информации. Модель нарушителя. Модель угроз. Категории мер защиты	2	
Лекция. Классификация, способы внедрения, признаки присутствия и технологии самозащиты вредоносного ПО. Методы обнаружения и защиты	2	
Лабораторная работа. Лабораторная работа №3. Сравнительный анализ понятийных аппаратов различных источников в области информационной безопасности	6	
Лабораторная работа. Лабораторная работа №4. Социальная коммуникация	6	
Задания для самостоятельной работы, в том числе выполнение Проработка лекций. Подготовка к лабораторным работам. Задания для самостоятельной работы.	18	
Политика уничтожения данных. Следы в сети. Принципы построения систем защиты информации	36	ОПК-6
Лекция. Уничтожение конфиденциальной информации (плановое и экстренное). Особенности удаления информации с электронных носителей. Необходимость уничтожения документов	2	
Лекция. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Конфиденциальность в социальных сетях	2	
Лекция. Классификация основных видов атак на компьютерные системы. Методы и средства обеспечения безопасности.	2	

Системы менеджмента информационной безопасности		
Лабораторная работа. Лабораторная работа №5. Информационная безопасность: логико-смысловая модель и основы криптографии	6	
Лабораторная работа. Лабораторная работа №6. Передача информации	6	
Задания для самостоятельной работы, в том числе выполнение КР Проработка лекций. Подготовка к лабораторным работам. Задания для самостоятельной работы.	18	
Иная контактная работа: выполнение контрольной работы	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины "Основы информационной безопасности" рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

Занятия лекционного типа дают систематизированные знания по дисциплине "Основы информационной безопасности", концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. Подготовка к **занятиям семинарского типа** включает ознакомление с планом лабораторного занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины "Основы информационной безопасности". Содержание **самостоятельной работы** определяется рабочей программой дисциплины "Основы информационной безопасности", оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины "Основы информационной безопасности", к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины "Основы информационной безопасности" включает выполнение контрольной работы и лабораторной работы. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине "Основы информационной безопасности" является экзамен.

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Основы информационной безопасности [Текст] : [учеб. пособие по специальностям в обл. информ. безопасности] / Е. Б. Белов [и др.]. М.: Горячая линия - Телеком, 2006. - 544 с. ISBN 5-93517-292-5. Экземпляры: всего 16.	16
2.	Основы информационной безопасности [Электронный ресурс] : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Москва: Горячая линия-Телеком, 2011. - 558 с. ISBN 5-93517-292-5.	https://e.lanbook.com/book/111016
3.	Бубнов, Алексей Алексеевич. Основы информационной безопасности [Текст] : учебник для среднего профессионального образования по специальности "Информационная безопасность" / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. 2-е изд., стер. Москва: Академия, 2019. - 253, [2] с. ISBN 978-5-4468-7763-8. Экземпляры: всего 25.	25
4.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2023. - 324 с. ISBN 978-5-8114-6738-9.	https://e.lanbook.com/book/341267
5.	Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 266 с. ISBN 978-5-94774-821-5.	https://e.lanbook.com/book/100295
6.	Фаронов, А. Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / Фаронов А. Е. 2-е изд. Москва: ИНТУИТ, 2016. - 154 с.	https://e.lanbook.com/book/100296
7.	Смирнов, Владимир Иванович. Защита информации [Текст] : лабораторный практикум : [по направлению 09.03.01] / В. И. Смирнов; М-во образования и науки Рос. Федерации, ФГБОУ ВО "Поволж. гос. технол. ун-т". Йошкар-Ола: ПГТУ, 2017. - 65 с. ISBN 978-5-8158-1866-8. Экземпляры: всего 24.	24 / https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	535 (III)	Ноутбук Acer (1), Персональный компьютер в сборе PowerCool(Core i3-8100/H310/16GbDDR4/HDD 0.5Tb/23"6 AOC/кл.мышь/пач-корд 3м) (20), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Microsoft Office Standard, Агент Dr.Web, Microsoft Visio Professional, Microsoft Visual Studio Enterprise,

			Комплект ПО для решения основных пользовательских задач, Справочная правовая система "Консультант Плюс", Комплект ГАРАНТ-Мастер
2.	107 (III)	Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Microsoft Office Standard, Агент Dr.Web, Microsoft Visio Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Справочная правовая система "Консультант Плюс", Комплект ГАРАНТ-Мастер

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает,	отлично

	дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	
--	--	--

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

1. Документированная информация –

- a) зафиксированная на материальных носителях информация
- b) зафиксированная на материальных носителях информация с реквизитами
- c) текст, напечатанный на бумаге
- d) текст, напечатанный на бумаге с реквизитами

2. Информационная война, в качестве основного объекта воздействия которой рассматриваются каналы связи между командованием и исполнителями

- a) командно-управленческая
- b) разведывательная
- c) хакерская
- d) психологическая

3. Основным органом, координирующим действия государственных структур по вопросам защиты государственной тайны, является

- a) ФСБ России
- b) Совет Безопасности Российской Федерации
- c) ФСТЭК России
- d) Межведомственная комиссия по защите государственной тайны

4. Приращение знаний возникающее в процессе взаимодействия самоуправляющейся системы с окружающей средой называется

- a) автономной информацией
- b) информацией воздействия
- c) информацией взаимодействия
- d) не знаю

5. Интеграция всех видов и направлений ИБ для достижения цели –

- a) структурная комплексность
- b) инструментальная комплексность
- c) функциональная комплексность
- d) временная комплексность

6. Что является продуктом информационной системы

- a) документ
- b) информационный ресурс
- c) информация
- d) сервис

7. Согласно статье 5 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ “Об информации, информационных технологиях и о защите информации”, информация в зависимости от категории доступа к ней подразделяется на ...

- a) общедоступную информацию и конфиденциальную информацию
- b) общедоступную информацию и информацию, доступ к которой ограничен федеральными законами
- c) интеллектуальную собственность и конфиденциальную информацию
- d) интеллектуальную собственность и информацию, доступ к которой ограничен федеральными законами

8. На базе среды Интернет с помощью специальных программ и технологий возможно создание искусственного общественного мнения. Существуют приложения, которые даже после смерти пользователя могут самостоятельно продолжать генерировать записи от его имени, а также публиковать ретвиты сообщений со страниц, которые он активно цитировал. О какой угрозе идёт речь?

- a) угроза астротерфинга
- b) угроза скулшутинга
- c) угроза рекрутинга
- d) угроза думскроллинга

9. Основные принципы обеспечения безопасности определяет действующий документ:

- a) Федеральный закон от 28 декабря 2010 года N 390-ФЗ "О безопасности"
- b) Закон Российской Федерации от 5 марта 1992 года N 2446-1 "О безопасности"
- c) Доктрина информационной безопасности Российской Федерации (5 декабря 2016 г.)
- d) Концепция национальной безопасности Российской Федерации (10 января 2000 г.)

10. Что является основной причиной старения информации?

- a) физическая изношенность носителя
- b) появление новой информации, с поступлением которой прежняя информация оказывается неверной
- c) устаревание знаковой системы, посредством которой выражена информация
- d) величина длительности хранения информации: чем больше длительность, тем информация старше

11. Назовите свойство данных, которое заключается в том, что время их сбора и переработки соответствует динамике изменения ситуации:

- a) идентичность
- b) оперативность

- c) адаптивность
- d) актуальность

12. На чем основывается политика информационной безопасности в организации?

- a) на выявлении всех возможных угроз информационной безопасности организации
- b) на поиске уязвимостей информационной системы организации
- c) на анализе рисков, признанных реальными для информационной системы организации
- d) на регистрации всех действий персонала при работе с защищаемой информацией

13. Уязвимость — это ...

- a) наличие узких мест в системе защиты информации
- b) слабость системы информационной безопасности
- c) незащищенность или ошибка в объекте, которая может привести к возникновению угрозы
- d) незащищенность объектов информационной системы

14. Неумышленное происшествие с деструктивным воздействием на объект

- a) ошибка
- b) катастрофа
- c) авария
- d) повреждение

15. Возможность за приемлемое время получить требуемую информационную услугу определяет ...

- a) пропускную способность канала
- b) время отклика системы
- c) качество сервиса
- d) степень доступности информации

16. Фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой информационной безопасности— это ...

- a) контроль
- b) учёт
- c) слежка
- d) регистрация

17. Субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы, — это ...

- a) вредитель
- b) хакер
- c) правонарушитель
- d) злоумышленник

18. Что относится к основной деятельности Минобороны России в области обеспечения информационной безопасности?

- a) разработка криптографических средств защиты информации
- b) организация деятельности по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах РФ
- c) организация деятельности государственной системы противодействия техническим разведкам на федеральном уровне
- d) техническая защита информации в аппаратах федеральных органов государственной власти

19. Базовый федеральный закон, регулирующий информационные отношения (в том числе

связанные с защитой информации) — это Федеральный закон:

- a) «Об информации, информационных технологиях и защите информации»
- b) «О коммерческой тайне»
- c) «О государственной тайне»
- d) «О безопасности критической информационной инфраструктуры Российской Федерации»

20. Степенью секретности информации не является:

- a) ограниченность в доступе
- b) особая важность
- c) совершенно секретно
- d) секретно

Перечень вопросов для проведения промежуточной аттестации

Вопросы на экзамен

1. Информация как фактор развития науки, техники и экономики. Специфика информации как товара.
2. Сущность конституционного права на информацию. Виды и свойства информации.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная). Цели и задачи защиты информации. Требования к системе защиты информации.
4. Предметная область комплекса наук о безопасности. Основные принципы обеспечения безопасности.
5. Полномочия Президента Российской Федерации в области обеспечения безопасности. Совет Безопасности Российской Федерации в государственной системе обеспечения национальной безопасности.
6. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Соотношение понятий «информационная безопасность» и «национальная безопасность».
7. Национальные интересы Российской Федерации и стратегические национальные приоритеты. Обеспечение национальной безопасности.
8. Государственная информационная политика. Технологический и содержательный аспекты государственной информационной политики.
9. Система обеспечения информационной безопасности Российской Федерации. Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации.
10. Обеспечение информационной безопасности: содержание и структура понятия. Основные понятия, общеметодологические принципы обеспечения информационной безопасности.
11. Доктрина информационной безопасности. Угрозы информационной безопасности Российской Федерации.
12. Важность защиты критической информационной инфраструктуры для обеспечения национальной безопасности Российской Федерации. Критические системы информационной инфраструктуры.
13. Понятие информационной войны. Цели информационной войны, её составные части и средства её ведения.
14. Информационные операции в ходе информационной войны. Психологические операции. Оперативная маскировка.
15. Возможные пути реализации информационной войны в современном мире. Уровни ведения информационной войны.
16. Информационная война и информационное оружие. Особенности технических средств информационной войны. Классификация средств защиты и нападения.
17. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники. Средства силового деструктивного воздействия (СДВ).
18. Общие принципы защиты информации. Безопасность (защищённость) компьютерных систем.
19. Модели управления доступом в компьютерных системах.
20. Категории мер защиты. Обзор средств и методов информационной/компьютерной безопасности.
21. Факторы, воздействующие на информацию.
22. Понятие угрозы информации. Виды угроз.
23. Источники угроз. Модель действий вероятного нарушителя и модель построения защиты. Исходные данные модели для внешнего и внутреннего нарушителя.

24. Уязвимость информационных систем.
25. Последствия реализации угроз. Классификация нарушений работоспособности АС по объектам воздействия и способам нанесения ущерба. Вывод АС из эксплуатации.
26. Методы нарушения конфиденциальности, целостности и доступности информации.
27. Моделирование угроз.
28. Угрозы утечки информации по техническим каналам.
29. Классы каналов несанкционированного получения информации.
30. Компьютерные вирусы как вид информационно-программного оружия. Признаки присутствия вредоносного ПО.
31. Классификация вредоносных программ. Способы внедрения.
32. Троянские программы, люки, эксплойты. Технологии самозащиты.
33. Задача антивирусной защиты. Методы защиты и обнаружения вредоносного ПО.
34. Задача антивирусной защиты. Классификация средств антивирусной защиты.
35. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ.
36. Межсетевое экранирование. Место и роль межсетевых экранов (МЭ) в обеспечении безопасности ресурсов АС.
37. Необходимость уничтожения документов. Особенности удаления информации с электронных носителей.
38. Политика уничтожения данных. Уничтожение конфиденциальной информации (плановое и экстренное).
39. Информационная безопасность и Интернет. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки".
40. Информационная безопасность и Интернет. Конфиденциальность в социальных сетях.
41. Классификация основных видов атак на компьютерные системы. Примеры сетевых атак.
42. Вычислительные сети как объект информационной безопасности. Базовая эталонная сетевая модель стека сетевых протоколов OSI.
43. Сетевая разведка. Оперативные средства и методы для нейтрализации атак.
44. Компьютерно-техническая экспертиза. Требования законодательства к методике производства экспертизы.
45. Системы менеджмента информационной безопасности. Основные требования. Политика безопасности организации.
46. Оценка рисков информационной безопасности от внешних и внутренних угроз. Управление рисками.
47. Системы защиты конфиденциальных данных от внутренних угроз.
48. Лицензирование и сертификация в области защиты информации.
49. Общая характеристика оценочных стандартов информационной безопасности.
50. Стандарты и спецификации в области информационной безопасности.