

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан РТФ

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

11.03.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

М.1.1.5 Обеспечение информационной безопасности в инфокоммуникациях

(код и наименование дисциплины по учебному плану)

Направление подготовки
(специальность)

27.04.04 Управление в технических системах

Квалификация выпускника

Магистр

(бакалавр/магистр/специалист)

Программа магистратуры

Искусственный интеллект в системах управления

Курс 1
Семестр 2

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	14	часов
Лабораторные работы	28	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	42	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	102	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	2	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 27.04.04 Управление в технических системах

Программу составили:

профессор, доктор наук	РТиС	СОГЛАСОВАНО	Н.В. Рябова
(должность)	(кафедра)		(И.О. Фамилия)
доцент	РТиС	СОГЛАСОВАНО	Р.Р. Бельгибаев
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра радиотехники и связи

(наименование кафедры)			
31.01.2024	протокол №	1	
(дата)			
Заведующий кафедрой	СОГЛАСОВАНО	Н.В. Рябова	
		(И.О. Фамилия)	

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

Заведующий кафедрой	СОГЛАСОВАНО	Т.С. Буканова
		(И.О. Фамилия)

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

СОГЛАСОВАНО	А.Н. Дедов
	(И.О. Фамилия)

Эксперт(ы): Бастраков Александр Владиславович, заместитель главного инженера АО
"ММЗ"

Рабочая программа проверена и зарегистрирована в УМЦ 12.03.2024 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-7 Способен осуществлять обоснованный выбор, разрабатывать и реализовывать на практике схемотехническое и аппаратно-программные решения для систем автоматизации и управления	ОПК-7.1. Использует схемотехнические, системотехнические и программно-аппаратные решения для систем автоматизации и управления	знания: Знать схемотехнические, системотехнические и программно-аппаратные решения для систем автоматизации и управления умения: Уметь применять типовые схемотехнические и программно-аппаратные решения для систем автоматизации и управления навыки: Владеть навыками выбора схемотехнических и программно-аппаратных решений для реализации систем автоматизации и управления
	ОПК-7.2 Осуществляет обоснованный выбор и реализацию системотехнических, схемотехнических, программно-аппаратных решений для систем автоматизации и управления	знания: Знать критерии выбора схемотехнических, схемотехнических, программно-аппаратных решений для систем автоматизации и управления умения: Умеет реализовывать схемотехнические, схемотехнические, программно-аппаратные решения для систем автоматизации и управления навыки: Владеет навыками разработки и практического применения схемотехнических, схемотехнических, программно-аппаратных решений для систем автоматизации и управления
	ОПК-7.3 Применяет современные информационно-коммуникационные технологии и интеллектуальные компьютерные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	знания: Знает современные информационно-коммуникационные технологии и интеллектуальные компьютерные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач умения: Умеет применять современные информационно-коммуникационные и интеллектуальные компьютерные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач навыки: Владеет навыками решения задач управления и автоматизации с использованием современных информационно-коммуникационных и интеллектуальных компьютерных технологий, инструментальных сред, программно-технических платформ

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: САПР в радиотехнике, электронике и связи (ОПК-7), Программно-технические средства автоматизации (ОПК-7)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих практиках: Преддипломная практика (ОПК-7), Производственная практика. Научно-исследовательская работа (рассредоточенная) (ОПК-7); государственной итоговой аттестации в форме: Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-7)

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 занятия, процедуры самообучения

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Защита информации. Основные понятия	42	ОПК-7
Лекция. Защита информации	2	
Лабораторная работа. Работа с программой Cisco Packet Tracer	6	
Задания для самостоятельной работы, в том числе выполнение Изучить рекомендованную литературу	34	
Алгоритмы шифрования данных	60	ОПК-7
Лекция. Алгоритмы шифрования данных. Перестановка	2	
Лекция. Шифры гаммирования	2	
Лабораторная работа. Моделирование процессов шифрования и дешифрования с помощью криптографического алгоритма замены	8	
Лекция. Алгоритмы шифрования данных. Подстановка	4	
Лабораторная работа. Моделирование процессов шифрования и дешифрования с помощью криптографического алгоритма перестановок	5	
Лабораторная работа. Моделирование процессов шифрования и дешифрования с помощью криптографического алгоритма гаммирования	5	
Задания для самостоятельной работы, в том числе выполнение Изучить рекомендованную литературу	34	
Информационная безопасность Применение систем искусственного интеллекта.	42	ОПК-7

Лекция. Информационная безопасность	2
Лекция. Применение систем искусственного интеллекта для обеспечения информационной безопасности	2
Лабораторная работа. Применение интеллектуального метода анализа данных в обеспечении информационной безопасности	4
Задания для самостоятельной работы, в том числе выполнение Изучить рекомендованную литературу	34
Иная контактная работа: консультации, дифференцированный зачет (БРК)	0

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины 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, 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.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины, 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, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины включает выполнение **лабораторной работы**. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине является БРК.

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.	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных [Текст] : Учеб.пособ.для студ-ов вузов,обуч.по	5

	<p>спец."Защищен.телекоммуникац.системы", "Комплекс.обеспечение инф.безопасности автоматизирован.систем" / [П.Ю.Белкин,О.О.Михальский,А.С.Першаков и др.]. М.: Радио и связь, 1999. - 168 с. ISBN 5-256-01416-1. Экземпляры: всего 5.</p>	
2.	<p>Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет- университет информ. технологий. М., 2003. - 277 с. ISBN 5-9556-0003-5. Экземпляры: всего 20.</p>	20
3.	<p>Конеев, Искандер Рустамович. Информационная безопасность предприятия [Текст] : [понятия и принципы. Методики и модели защиты. Классификация атак. Типовая модель нападения. Немного о хакерах и анонимайзерах. Методика упр. рисками. Критерии оценки. Криптогр. средства и механизмы. Истории криптогр. Классификация шифров] / И. Конеев, А. Беляев. Санкт-Петербург: БХВ-Петербург, 2003. - 733 с. ISBN 5-94157-280-8. Экземпляры: всего 10.</p>	10
4.	<p>Соболев, Анатолий Николаевич. Физические основы технических средств обеспечения информационной безопасности [Текст] : [учеб. пособие для студентов вузов по специальностям 075500 "Комплексное обеспечение информ. безопасности автоматизир. систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. М.: Гелиос АРВ, 2004. - 221 с. ISBN 5-85438-084-6. Экземпляры: всего 47.</p>	46
5.	<p>Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет-университет информ. технологий. 2-е изд., испр. М., 2004. - 261 с. ISBN 5-9556-0015-9. Экземпляры: всего 23.</p>	23
6.	<p>Рябова, Наталья Владимировна. Защита информации в радиотехнических, вычислительных системах и сетях [Текст] : лаб. практикум / Н. В. Рябова. Йошкар-Ола: МарГТУ, 2005. - 46 с. Экземпляры: всего 71.</p>	71
7.	<p>Кубашева, Елена Сергеевна. Информатика и вычислительная техника. Информационная безопасность автоматизированных систем [Текст] : учебно-методическое пособие к прохождению производственной практики для студентов направлений подготовки 09.03.01 "Информатика и вычислительная техника", 10.05.03 "Информационная безопасность автоматизированных систем" / Е. С. Кубашева, И. А. Малашкевич, Е. Н. Чекулаева; Министерство науки и высшего образования Российской Федерации, ФГБОУ ВО "Поволжский государственный технологический университет". Йошкар-Ола: ПГТУ, 2019. - 64, [1] с. ISBN 978-5-8158-2081-4. Экземпляры: всего 23.</p>	<p>23 / https://portal.volgatech.net/books/Kubacheva_Informatika_i_vichislitelnaai_tehnika_Informazionnaai_bezopasnost_avtomatizirovannih_sistem_2019.pdf</p>
8.	<p>Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2023. - 324 с. ISBN 978-5-8114-6738-9.</p>	<p>https://e.lanbook.com/book/341267</p>

9.	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
10.	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
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru

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.	333г (III)	Компьютер P4-3.0/2*256Mb/HDD 200Gb/128 6600GT/DVD-RW/KM/FDD/MBi945P/UPS (1), Монитор 19"Samsung 940N (LKSB) TFT (1), Комплект учебной мебели (1)	Microsoft Office Standard, Комплект ПО для решения основных пользовательских задач, Mathcad University Classroom Perpetual - 40, Агент Dr.Web

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	отлично

	материал, грамотно и логически стройно его излагает, 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 проектных 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 Какой из следующих протоколов представляет из себя протокол, обеспечивающий только управление передачей данных?

TCP.

IP.

TCP/IP.

ATM.

2 Какая из следующих технологий предназначается для работы с частными виртуальными сетями?

VPN.

FrameRelay.

IP.

ISO.

3 Сетевой уровень системы OSI выполняет функцию

Задаёт передаваемым данным адрес узла назначения и узла источника.

Осуществляет передачу потока битов по физической среде.

Формирует кадры данных из пакетов данных.

Устанавливает сеанс связи между двумя конечными узлами.

4 Сколько уровней насчитывает модель открытой системы Open System Interconnection

- 7.
- 10.
- 5.
- 9.

5 Схема Router->Switch->Hub соответствует уровням модели Open System Interconnection в следующем порядке

- Сетевой-> Канальный -> Физический
- Транспортный ->Канальный ->Физический
- Транспортный -> Сетевой -> Канальный
- Сеансовый -> Сетевой->Физический

6 Какое утверждение о функциях стоп бита в кадре данных является верным ?

- стоп бит всегда удаляется после приёма.
- стоп бит всегда является лог. Единицей.
- стоп бит всегда является лог. Нулём.
- стоп бит всегда дополняется чётным битом после приёма.

7 Статические IP адреса желательно назначать на оборудование ?

- всё вышеперечисленное.
- маршрутизатор, сетевой принтер.
- сервер, сетевой принтер.
- маршрутизатор, сервер.

8 для Маски типа 11111111 11111111 11111110 00000000 возможно следующее максимальное количество узлов абонентов

- 510
- 255
- 130
- 100000000

9 Какой топологии сетей не существует ?

- Тройная шинная топология
- Расширенная звезда
- Иерархическая топология
- Полносвязная топология

10 Защита информации – это

- Комплекс мероприятий, направленных на обеспечение информационной безопасности.
- Своевременная ликвидация и шифрование архивных данных.
- Обеспечение контроля санкционированности операций с банком данных.

- Соккрытие важной информации от рядовых сотрудников.

11 Спектр интересов субъектов, связанных с использованием информационных систем, не подразумевает свойство ?

- эквивалентности.

- доступности.

- целостности.

- конфиденциальности.

12 Наиболее опасные угрозы информационной безопасности

- внутренние угрозы.

- внешние угрозы.

- ЭМ импульсы.

- вирусные атаки.

13 Искжением информации не является ?

- нарушение конфиденциальности информации

- саботаж

- мошенничество

- сбой в работе информационной системы.

14 Какое из следующих утверждений про автоматизированную систему обработки информации верно?

- Безопасность АСОИ – свойство защищенности системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.

- Безопасность АСОИ достигается принятием мер по обеспечению узкого круга лиц работающих с АСОИ

- Под угрозой безопасности АСОИ понимаются возможные воздействия на АСОИ, которые прямо или косвенно могут нанести ущерб ее безопасности.

- Комплекс средств защиты - средства пожаротушения, создаваемых и поддерживаемых для обеспечения безопасности АСОИ.

15 автоматизированная система обработки информации не состоит из следующего компонента ?

- передвижного пункта сбора информации

- персонал

- данные

- аппаратные средства

16 Ошибки в работе обслуживающего персонала и пользователей; помехи в линиях связи из-за воздействий внешней среды являются примерами

- случайные воздействия

- преднамеренные воздействия

- аппаратные воздействия
- человеческое воздействие

17 некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы

- Уязвимость АСОИ
- Ущерб безопасности АСОИ
- Политика безопасности
- Несанкционированный доступ

18 Активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы - это ... ?

- Субъект
- Объект
- Администратор
- Средства контроля доступа

19 К основным путям реализации угроз безопасности АСОИ при воздействии на ее компоненты типа: Персонал, не относится ?

- НСД-подключение; использование ресурсов; модификация, изменение режимов
- Разглашение: передача сведений о защите; халатность.
- «Маскарад»; вербовка; подкуп персонала
- Уход с рабочего места; физическое устранение

20 Выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

- «Маскарад»
- Сетевой «червь»
- Активное вторжение
- Пассивное вторжение

21 Группу важнейших понятий объектного подхода не составляет

- детализация,
- инкапсуляция,
- наследование,
- полиморфизм.

22 Понятие «полиморфизм» подразумевает

- Способность объекта принадлежать более чем одному классу
- Скрытие реализации объектов с предоставлением вовне только строго определенных интерфейсов.
- Изменение или добавление правильного или ложного сообщения

- Построение абстракций разных моделируемых предметных областей

23 Одной из основных граней информационной безопасности является

- целостность
- наследование
- полиморфизм
- инкапсуляция

24 Традиционный подход к информационной безопасности с объектной точки зрения устарел, так как

- В объектном подходе пассивных объектов нет
- Увеличивая уровень детализации, можно разглядеть не только разнесенные производственные площадки, но и каналы связи между ними
- Конкретизация направленности, с учетом наличия внешнего подключения, должна быть выполнена на административном, процедурном и программно-техническом уровнях.
- Возможно, какую-либо информацию нельзя хранить и обрабатывать на компьютерах

25 Основной функцией безопасности современных ОС становится

- защита возможностей, предоставляемых привилегированным пользователям
- контролирует объекты, с которыми работают пользователи
- контролирует действия пользователей, которые регистрируются и учитываются прикладными средствами
- Для каждого приложения создают виртуальный контейнер.

26 Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется

- окно опасности
- доминирующего средства безопасности
- разграничение доступа
- семантика действия

27 применительно к пользователям не рассматривается следующая угроза

- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий
- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности)
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности)
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации)

28 Основными источниками внутренних отказов не является:

- разрушение или повреждение помещений;
- отказы программного и аппаратного обеспечения

- разрушение данных

- разрушение или повреждение аппаратуры

29 атака, получившая наименование «DoS– атака» является

- программных атаках на доступность

- физических атак на доступность

Атак пользователей на доступность

Всё вышеперечисленное

30 обычно осуществляющую разрушительную функцию ПО не предназначаются для

производства резервного копирования данных

получения контроля над атакуемой системой

агрессивного потребления ресурсов

внедрения другого вредоносного ПО

31 Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах

Программный вирус

троянский вирус

сетевой червь

фишинговая ссылка

32 ошибки типа «переполнение буфера», используются в

Для внедрения осуществляющую разрушительную функцию ПО

Для обнаружения в коде сетевого червя

Для обнаружения в коде троянского вируса

агрессивного потребления ресурсов

33 Угрозами динамической целостности не является

ввод неверных данных

нарушение атомарности транзакций

переупорядочение, кража, дублирование данных

внесение дополнительных сообщений (сетевых пакетов и т.п.)

34 в меры для защиты интересов субъектов информационных отношений не входит

Метод хранения

Законодательный

Административный

Процедурный

35 гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений статья

23 статья

41 статья

42 статья

29 статья

36 Федеральным законом о защите персональных данных является закон под номером N 152-ФЗ

N 126-ФЗ

N 142-ФЗ

N 116-ФЗ

37 Глава 28 УК РФ -«Преступления в сфере компьютерной информации»-содержит

три статьи

четыре статьи

шесть статей

пять статей

38 Статья 274 УК РФ говорит о

Нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети

Неправомерного доступа к компьютерной информации

Создании, использовании и распространении вредоносных программ для ЭВМ

О случаях, когда информация составляет служебную или коммерческую тайну

39 Статья 138 УК РФ затрагивает тему

Предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Создание, использование и распространение вредоносных программ для ЭВМ

Соккрытие достоверной информации о состоянии окружающей среды

40 защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности называются

Гостайна

Персональные данные

Секретная информация

Особо важная информация

41 Закон «О государственной тайне» даёт определение следующему понятию

Средства защиты информации

Персональные данные

Неправомерный доступ

Конфиденциальная информация

42 Закон «Об информации, информатизации и защите информации» имеет в глоссарии определение

Информационные ресурсы

Средства защиты информации

Гостайна

Правила эксплуатации ЭВМ

43 Закон «Об информации, информатизации и защите информации» имеет в глоссарии определение

Конфиденциальная информация

Гостайна

Злоупотребление полномочиями

Средства защиты информации

44 Закон «Об информации, информатизации и защите информации» имеет в глоссарии определение не выделяет следующий параграф защиты информации, как цель

Создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности

Предотвращение угроз безопасности личности, общества, государства

Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах

Сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

45 специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное специальным органом юридическому лицу или индивидуальному предпринимателю

Лицензия

Патент

Договор

Диплом

46 Юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности

Лицензиат

Лицензирующий орган

Лицензирование

Лицензия

47 Основными лицензирующими органами в области защиты информации являются

ФАПСИ, Гостехкомиссия

Гостехкомиссия, Роскомнадзор

Роскомнадзор, ГРЧЦ

ГРЧЦ, ФАПСИ

48 Корпоративная информационная система

Информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы

Физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи

Положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи

Информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано

49 Основными направлениями деятельности на законодательном уровне не является

необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами

разработка новых законов с учетом интересов всех категорий субъектов информационных отношений

интеграция в мировое правовое пространство

учет современного состояния информационных технологий

50 Во второй уровень детализации информационной системы не входит:

Сервисы, используемые организацией

Представляемые сервисы

Пользователи внутренних сервисов

Внутренние сервисы

51 Мера доверия, которая может быть оказана архитектуре и реализации ИС – это...

Уровень гарантированности

Политика безопасности

Доверенная вычислительная база

Безопасность повторного использования объектов

52 В «Оранжевой книге» уровень доверия ... имеет так же и классы доверия

Уровень доверия В

Уровень доверия D

Уровень доверия E

Уровень доверия А

53 На каком уровне эталонной семиуровневой модели OSI не возможно реализовать не одну из представленных ниже функций безопасности

5й уровень

7й уровень

3й уровень

2й уровень

54 Согласно рекомендациям X.800, аутентификация не может достигаться за счет использования ... личности получателей.

Паролей

Устройств измерения

криптографических методов

55 С какими механизмами безопасности не предназначена для реализации функция безопасности «Неотказуемость»

Шифрование, Дополнение трафика

Шифрование, Электронная подпись

Целостность, Электронная подпись

Аутентификация, Целостность

56 механизм «Электронная подпись» пригоден для реализации данной выборке функции безопасности

Аутентификация источника, неотказуемость, целостность вне соединения

Целостность вне соединения, аутентификация источника, конфиденциальность трафика

Управление доступом, аутентификация источника, избирательная конфиденциальность

Управление доступом, избирательная конфиденциальность, конфиденциальность трафика

57 содержит совокупность требований к конкретно разработке, выполнение которых обеспечивает достижение поставленных целей безопасности:

Задание по безопасности

Профиль защиты

Компонент безопасности

Профиль безопасности

58 Требования доверия безопасности: анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование, предусматривает?

уровень доверия 1

уровень доверия 2

уровень доверия 3

уровень доверия 4

59 Требования доверия безопасности: контроль среды разработки и управление конфигурацией объекта оценки, предусматривает?

уровень доверия 3

уровень доверия 1

уровень доверия 2

уровень доверия 4

60 В жизненном цикле информационного сервиса на этапе ... происходят мероприятия - составляются спецификации, прорабатываются варианты приобретения?

Закупка

Установка

Инициация

Выведение из эксплуатации

Перечень вопросов для проведения промежуточной аттестации

1. Показатели эффективности систем защиты.
2. Политика безопасности в компьютерных сетях.
3. Управление доступом в компьютерных сетях.
4. Многоуровневая защита корпоративных сетей.
5. Механизмы защиты операционных сетей.
6. Отказоустойчивость, интенсивность отказов, время наработки на отказ.
7. Время восстановления системы защиты, коэффициент готовности.
8. Соперничество в информационной сфере; информационные войны.
9. Информационная безопасность в бизнесе.ttt
10. Информационные права граждан.
11. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
12. Анализ компьютерных преступлений
13. Методы сбора сведений для вторжения в сеть
14. Модель нарушителя безопасности информации
15. Способы несанкционированного доступа к информации через технические средства, к проводным линиям связи, к волоконно-оптическим линиям связи, к беспроводным линиям связи
16. Технология беспроводной связи Bluetooth

17. Контроль мобильных средств связи
18. Шпионские программные закладки
19. Программы обнаружения сетевых атак
20. Защита сети с помощью биометрических систем
21. Основные положения и определения криптографии
22. Принципы построения компьютерной стеганографии
23. Нейронная сеть (Neural network)
24. Машинное обучение (Machine learning)
25. Большие данные (Big Data)
26. Глубокий анализ данных (Data mining)
- 27.