

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

02.02.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.37 Организация защиты информационных систем

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника Специалист
(бакалавр/магистр/специалист)

Специализация Анализ безопасности информационных систем

Курс 4
Семестр 8

Распределение учебного времени

Трудоемкость по учебному плану	180 / 5	часов/зачетных единиц
Лекции	32	часов
Лабораторные работы	32	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	64	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	80	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	8	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:

доцент	ИБ	СОГЛАСОВАНО	А.П. Александров
(должность)	(кафедра)		(И.О. Фамилия)

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

(наименование кафедры)		
31.01.2022	протокол №	23
(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 07.02.2022 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. ПК-2 Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации	ПК-2.1.1 знает технические средства контроля эффективности мер защиты информации	знания: Виды информационных воздействий и критерии оценки защищенности информации в автоматизированных системах умения: навыки:
	ПК-2.1.2 знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем	знания: Принципы формирования политики информационной безопасности в автоматизированных системах умения: навыки:
	ПК-2.2.1 умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	знания: умения: Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы навыки:
	ПК-2.2.2 умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	знания: умения: Определять информационную инфраструктуру и информационные ресурсы автоматизированной системы, подлежащие навыки:
	ПК-2.3.1 Выполнение контрольных проверок работоспособности и эффективности систем и средств защиты информации	знания: Нормативные правовые акты в области защиты информации умения: Выявлять известные уязвимости информационных систем навыки: Проведение оценки качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения системы защиты информации
2. ОПК-17 Способен использовать программные и программно-аппаратные	ОПК-17.1 знает программно-аппаратные средства обеспечения защиты информации автоматизированных	знания: Основны меры по защите информации в автоматизированных системах умения: навыки:

средства для моделирования и испытания систем защиты информационных систем	ОПК-17.2 умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	знания: умения: Определять комплекс мер для обеспечения безопасности информации в автоматизированных системах навыки:
	ОПК-17.3 владеть навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах	знания: умения: навыки: Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы

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: Организация ЭВМ и вычислительных систем (ПК-2); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-17)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ПК-2), Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-17)

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

На достижение конкретных целей обучения направлены применяемые тактические технологии: классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

8 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Аудиторная и самостоятельная работа	144	ПК-2
Лекция. Темы лекций: 1. Концептуальные положения организационного обеспечения	32	

<p>информационной безопасности информационных систем.</p> <p>2. Организация службы безопасности объектов информатизации.</p> <p>3. Подбор и работа с кадрами на объекте информатизации.</p> <p>4. Организация и обеспечение режима защиты информации ограниченного доступа.</p> <p>5. Организация внутриобъектового и пропускного режима.</p> <p>6. Охрана объектов информатизации.</p> <p>7. Организация защищенного документооборота.</p> <p>8. Организация контроля работоспособности и эффективности системы информационной безопасности.</p>	
<p>Лабораторная работа. Лабораторные (практические) занятия:</p> <p>1. Угрозы безопасности информационной системе.</p> <p>2. Организационные меры по защите информационной системы.</p> <p>3. Структура службы информационной безопасности, ее задачи и функции.</p> <p>4. Разработка нормативных документов, регламентирующих деятельность службы информационной безопасности.</p> <p>5. Выбор мер по защите информации в информационной системе.</p> <p>6. Требования по защите государственных информационных систем.</p> <p>7. Организация защищенного документооборота информационной системы.</p> <p>8. Формы и способы контроля безопасности информационной системы</p>	32

<p>Задания для самостоятельной работы, в том числе выполнение РГР</p> <p>Темы РГР:</p> <ol style="list-style-type: none"> 1. Модель угроз информационной безопасности. Принципы построения модели угроз. 2. Модель нарушителя информационной безопасности. 3. Оценка ущерба, нанесенного объекту вследствие организационных нарушений информационной безопасности. 4. Организация и порядок проведения служебного расследования по фактам нарушения информационной безопасности. 5. Концепция безопасности информационной системы. 6. Организация контроля за соблюдением требований информационной безопасности. 7. Охранные организации, функции и задачи. Требования к их сотрудникам. 8. Организация охраны объекта. Системы видеонаблюдения. 9. Организация охраны объекта. Системы контроля и управления доступом. 10. Организация охраны объекта. Системы пожарно-охранной сигнализации. 11. Организация охраны объекта. Частное охранное предприятие. 12. Организация охраны объекта. Использование служебных собак. 13. Организация охраны объекта. Порядок использования оружия. 14. Организация охраны объекта. Средства индивидуальной защиты сотрудников подразделений охраны от оружия нападения. 15. Организация охраны объекта. Системы периметровой сигнализации. 16. Организация охраны объекта. Системы идентификации личности по биометрическим данным. 17. Организация внутриобъектового и пропускного режима. Цели и задачи внутриобъектового и пропускного режима. 18. Роль персонала в обеспечении информационной безопасности объекта. 19. Человеческий фактор как угроза информационной безопасности. 20. Порядок организации службы безопасности объекта информатизации. Основные документы, регламентирующие деятельность службы безопасности. 21. Государственные информационные системы. Требования по защите государственных информационных систем. 22. Организация защиты коммерческой тайны. 23. Организация защиты персональных данных. 24. Порядок работы со сведениями конфиденциального характера. 25. Организация защиты сведений служебного характера (служебной тайны). 26. Защищенный документооборот, организация защищенного 	
---	--

документооборота.		
27. Организация допуска и доступа должностных лиц к защищаемым сведениям.		
28. Критическая информационная система Российской Федерации. Объекты и субъекты КИИ.		
29. Категорирование объектов КИИ. Обеспечение безопасности значимых объектов КИИ.		
30. ГосСОПКА, основные понятия, функции, структура, взаимодействие с объектами КИИ.	80	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

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 практического (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, **расчётно-графической работы**.

Подготовка расчётно-графических работ осуществляется в течение семестра в соответствии с перечнем рекомендуемых тем РГР. Успешное выполнение РГР достигается путем анализа теоретических и практических материалов по выбранной теме тщательной подготовке к защите РГР.

Подготовка к выполнению РГР

Подготовка заключается в:

- внимательном изучении выбранной темы, уяснении цели и задачи работы;
- изучении и анализе относящихся к данной теме организационно-правовых документов и материалов их практического применения.

Выполнение РГР

Используя лекционный материал, действующие в Российской Федерации нормативно-правовые документы, регламентирующие деятельность в сфере информационной безопасности, учебную и специальную литературу,

информацию из современных периодических изданий подобрать материалы, необходимые для выполнения РГР. В работе могут приводиться примеры применения организационно-правовых и технических мер защиты информации по выбранной теме на российских предприятиях и в учреждениях, зарубежный опыт работы в данной области информационной безопасности, мнения о дальнейшем совершенствовании защиты информации в рассматриваемой области.

Целью выполнения РГР является формирование и развитие профессиональных компетенций, приобретение практических навыков реализации требований по организации защиты информации, изучение современного опыта построения систем информационной безопасности, подготовка к экзамену по результатам изучения дисциплины.

Оформление РГР

Составление отчета о проведенных исследованиях является заключительным этапом выполнения РГР. Отчет выполняется в электронном (машинописном) виде, руководствуясь следующими положениями:

- титульный лист оформляется в соответствии с требованиями по оформлению практических заданий и курсовых работ с указанием дисциплины и темы РГР;
- РГР должна содержать оглавление, введение с постановкой задачи, аналитическую часть, практическое использование/применение рассматриваемой темы, заключение, перечень используемой литературы. Допускается введение в РГР других разделов и приложений по усмотрению студента. Объем РГР как правило должен составлять 15-30 листов формата А-4;
- к защите РГР готовится презентация, состоящая из 10-15 слайдов.

Защита РГР проводится индивидуально.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине 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.	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
2.	Галатенко, В. А. Стандарты информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 307 с. ISBN 5-9556-0053-1.	https://e.lanbook.com/book/100511
3.	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 25.	25 / https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf
4.	Чекулаева, Елена Николаевна. Управление	15 /

	информационной безопасностью [Текст] : учебное пособие : для студентов и магистрантов направлений подготовки 10.05.03 "Информационная безопасность автоматизированных систем", 10.04.01 "Информационная безопасность" / Е. Н. Чекулаева, Е. С. Кубашева; Министерство науки и высшего образования Российской Федерации, ФГБОУ ВО "Поволжский государственный технологический университет". Йошкар-Ола: ПГТУ, 2020. - 153 с. ISBN 978-5-8158-2165-1. Экземпляры: всего	https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf
5.	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
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.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.	535 (III)	Ноутбук Acer (1), Персональный компьютер в сборе PowerCool(Core i3-8100/H310/16GbDDR4/HDD 0.5Tb/23"6 АОС/кл.мышь/пач-корд 3м) (20), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Microsoft Office Standard, Агент Dr.Web, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Справочная правовая система "Консультант Плюс"

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, 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	отлично

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.

**Образец
экзаменационного билета**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

По дисциплине: «Организация защиты информационных систем»

- 1. Структура сил и средств организационной защиты информации.**
- 2. Понятие пропускного режима. Цели и задачи пропускного режима.**

Зав. кафедрой ИБ _____ И.Г. Сидоркина

«__» _____ 20__ г.

Перечень вопросов для проведения промежуточной аттестации

Перечень

вопросов к экзамену

1. Виды угроз информационной безопасности информационной системе, их характеристика.
2. Принципы построения модели угроз и нарушителя информационной системы.
3. Формы и виды противоправных действий нарушителей информационной безопасности.
4. Оценка ущерба, нанесенного объекту вследствие нарушений информационной безопасности.
5. Основные направления и принципы организационной защиты информационной системы.
6. Структура сил и средств организационной защиты информации.
7. Охранные организации Российской Федерации, их функции и задачи.
8. Функции, задачи и особенности построения службы безопасности объекта информатизации.
9. Порядок организации службы безопасности объекта. Типовая структура службы безопасности объекта.
10. Основные документы, регламентирующие деятельность службы безопасности объекта.
11. Требования к сотрудникам объекта, допущенным к защищаемой информации. Их права и обязанности по защите информации.

12. Основные критерии приема на работу, связанную с сохранением тайны.
13. Состав документов, необходимых при подборе и приеме сотрудников, допускаемых к работе с защищаемой информацией.
14. Методы проверки кандидатов для работы с защищаемой информацией.
15. Организация контроля выполнения сотрудниками требований режима защиты информации.
16. Цели, задачи и процедура служебного расследования нарушений режима защиты информации.
17. Меры по защите информации при увольнении сотрудника.
18. Требования при организации защищенного документооборота.
19. Назначение и задачи защищенного делопроизводства.
20. Порядок разработки, учета, хранения, размножения и уничтожения защищенных документальных материалов.
21. Требования по организации защищенного документооборота с применением средств вычислительной техники.
22. Организация допуска и доступа работников к защищаемой информации.
23. Назначение и требования внутриобъектового режима.
24. Организация допуска сотрудников и посетителей на охраняемую территорию, в помещения защищаемых информационных систем.
25. Определение перечня предметов, запрещенных к проносу-провозу на территорию объекта информатизации.
26. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения.
27. Цели и задачи охраны. Объекты охраны.
28. Виды и способы охраны. Взаимодействие охраны с органами правопорядка.
29. Средства и методы физической защиты объектов.
30. Инженерно-технические средства охраны.
31. Назначение и требования к системам охранно-пожарной сигнализации на объектах информатизации.
32. Назначение и особенности применения систем охранного телевидения на объектах информатизации.
33. Системы контроля и управления доступом, их интеграция с другими техническими средствами охраны.
34. Системы идентификации личности по биометрическим данным. Особенности их использования для обеспечения безопасности информационных систем.
35. Понятие пропускного режима. Цели и задачи пропускного режима.
36. Организация пропускного режима.
37. Виды пропусков. Порядок оформления и выдачи пропусков.
38. Требования по защите значимых объектов критической информационной инфраструктуры.
39. ГосСОПКА, основные понятия, функции, структура.
40. Контроль эффективности системы информационной безопасности. Методы и формы контроля.

