

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

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

03.02.2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

С.1.1.34 Организационное и правовое обеспечение 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	4
Семестр	7

**Распределение учебного времени**

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	36	часов
Лабораторные работы	-	часов
Практические занятия	36	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	72	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	72	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	7	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)
заведующая кафедрой	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)

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

(наименование кафедры)			
31.01.2023	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 07.02.2023 г.  
Специалист учебно-методического центра СОГЛАСОВАНО /М.Л. Бойкова/

## 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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации	<b>знания:</b> знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации <b>умения:</b> <b>навыки:</b>
	ОПК-5.2 умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	<b>знания:</b> <b>умения:</b> умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы <b>навыки:</b>
	ОПК-5.3 Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	<b>знания:</b> Знает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов <b>умения:</b> Умеет разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов <b>навыки:</b> Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов
2. ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	ОПК-6.1 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	<b>знания:</b> знает основные угрозы безопасности информации и модели нарушителя объекта информатизации <b>умения:</b> <b>навыки:</b>
	ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	<b>знания:</b> <b>умения:</b> умеет разрабатывать модели угроз и модели нарушителя объекта информатизации <b>навыки:</b>

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	<b>знания:</b> Знает комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем <b>умения:</b> Умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации <b>навыки:</b> 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: Основы информационной безопасности (ОПК-6)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Управление информационной безопасностью (ОПК-5), Теоретические основы компьютерной безопасности (ОПК-6); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-5), 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 занятия, процедуры самообучения

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

## Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 7 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Аудиторная и самостоятельная работа</b>	<b>144</b>	ОПК-5, ОПК-6
Лекция. Темы лекций: 1. Основы обеспечения безопасности КИИ Российской Федерации. 2. Субъекты и объекты КИИ, их права и обязанности. 3. Категорирование объектов КИИ 4. Обеспечение безопасности значимых объектов КИИ	36	

<p>5. Контроль за обеспечением безопасности значимого объекта КИИ</p> <p>6. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)</p> <p>7. Аудит безопасности критической инфраструктуры.</p> <p>8. Юридическая ответственность за нарушения обеспечения безопасности КИИ</p> <p>9. Сравнительный анализ подходов к регулированию</p>		
<p>Практическое занятие. Лабораторные работы:</p> <p>1. Основы обеспечения безопасности КИИ Российской Федерации.</p> <p>2. Правила категорирования объектов КИИ.</p> <p>3. Подготовка исходных данных для категорирования объектов КИИ. Определение принадлежности к субъектам КИИ.</p> <p>4. Перечень показателей критериев ЗОКИИ и их значения. Оценка в соответствии с перечнем показателей критериев ЗОКИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.</p> <p>5. Категорирование объектов критической информационной инфраструктуры.</p> <p>6. Оформление и передача в ФСТЭК России результатов категорирования</p> <p>7. Требований по обеспечению безопасности значимых объектов КИИ РФ.</p> <p>8. Система безопасности значимого объекта КИИ.</p> <p>9. Организационные меры по обеспечению безопасности значимого объекта КИИ. Внедрение организационных мер.</p> <p>10. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ</p> <p>11. Контроль за обеспечением безопасности значимого объекта КИИ</p> <p>12. Перечень информации, представляемой в ГосСОПКА и Порядок представления информации в ГосСОПКА.</p> <p>13. Этапы проведения аудита. Практические особенности проведения аудита КИИ.</p> <p>14. Тестирование как один из основных типов аудита критической информационной инфраструктуры</p> <p>15. Тестирование критической инфраструктуры специальными информационно-психологическими воздействиями.</p> <p>16. Сравнительный анализ подходов к регулированию критической информационной инфраструктуры других стран</p>	36	

Задания для самостоятельной работы, в том числе выполнение РГР

Темы РГР:

1. Правовые основы обеспечения безопасности критической информационной структуры Российской Федерации.
2. Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ
3. Зарубежное нормативное регулирование защиты объектов КИИ.
4. Организационная система обеспечения безопасности критической информационной структуры Российской Федерации.
5. Субъекты КИИ, понятие, определение принадлежности, права и обязанности.
6. Объекты КИИ. Типы и виды объектов КИИ.
7. Категорирование объектов КИИ, понятие, общий порядок.
8. Комиссия по категорированию, порядок создания и деятельности комиссии.
9. Перечень критических процессов субъекта КИИ, порядок формирования перечня.
10. Перечень объектов КИИ, подлежащих категорированию.
11. Процедура категорирования объекта КИИ.
12. Определение категории значимости объекта КИИ.
13. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ.
14. Источники угроз объекту КИИ, способы реализации их, последствия.
15. Уязвимости объектов КИИ, классификация уязвимостей.
16. Типовые способы реализации угроз и компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
17. Методы оценки возможных последствий реализации возникновения угроз безопасности информации значимого объекта КИИ.
18. Алгоритм создания и функционирования СОИБ значимого объекта КИИ.
19. Основные требования по обеспечению безопасности значимого объекта КИИ.
20. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.
21. Требования к организационным и техническим мерам, направленным на блокирование (нейтрализацию) угроз безопасности информации значимого объекта КИИ.
22. Цели и задачи системы безопасности значимого объекта КИИ. Требования к их созданию.
23. Структура системы безопасности значимых объектов КИИ. Требования к силам обеспечения безопасности.
24. Основные документы системы безопасности значимых объектов КИИ и обеспечения их функционирования.

25. Этапы работ по созданию систем безопасности значимого объекта КИИ.		
26. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ.		
27. Виды контроля (мониторинга) за обеспечением уровня безопасности значимого объекта КИИ и его системы безопасности.		
28. Анализ и документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ.		
29. Федеральные органы исполнительной власти Российской Федерации, уполномоченные в области обеспечения безопасности КИИ, их функции.		
30. Ответственность за преступления и правонарушения в области защиты КИИ.	72	
Иная контактная работа:	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 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

- 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 готовиться 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 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
<b>УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ</b>		
1.	Прохорова, О. В. Информационная безопасность и	

	защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	<a href="https://e.lanbook.com/book/293009">https://e.lanbook.com/book/293009</a>
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.	<a href="https://e.lanbook.com/book/100511">https://e.lanbook.com/book/100511</a>
3.	Анисимов, А. А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / Анисимов А. А. 2-е изд. Москва: ИНТУИТ, 2016. - 212 с. ISBN 978-5-9963-0237-6.	<a href="https://e.lanbook.com/book/100636">https://e.lanbook.com/book/100636</a>
4.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2023. - 324 с. ISBN 978-5-8114-6738-9.	<a href="https://e.lanbook.com/book/341267">https://e.lanbook.com/book/341267</a>
5.	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 / <a href="https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf">https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf</a>
6.	Чекулаева, Елена Николаевна. Управление 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	15 / <a href="https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf">https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf</a>
7.	Белов, Евгений Борисович. Организационно-правовое обеспечение информационной безопасности [Текст] : учебник для среднего профессионального образования по специальности "Информационная безопасность". Номер рецензии Р118/1 от 1 августа 2019 г. / Е. Б. Белов, В. Н. Пржегорлинский. 2-е изд., испр. и доп. Москва: Академия, 2020. - 332, [1] с. ISBN 978-5-4468-8456-8. Экземпляры: всего 24.	24
<b>ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ</b>		
1.	Научная электронная библиотека eLIBRARY.RU	<a href="http://elibrary.ru">http://elibrary.ru</a>
2.	Научная электронная библиотека «Киберленинка»	<a href="http://cyberleninka.ru">http://cyberleninka.ru</a>
<b>ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ</b>		
1.	Справочно-правовая система Консультант+	<a href="http://www.consultant.ru">http://www.consultant.ru</a>
2.	Информационно-правовой портал Гарант	<a href="http://www.garant.ru">http://www.garant.ru</a>

## 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, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач

## 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	отлично

	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	
--	--	--

### 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.

## МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

## ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

По дисциплине: «Организация защиты объектов критической информационной структуры»

### 1. Объекты и субъекты КИИ.

### 2. Структура системы безопасности значимых объектов КИИ.

Зав. кафедрой ИБ \_\_\_\_\_ И.Г. Сидоркина

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

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

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**

По дисциплине: «Организация защиты объектов критической информационной структуры»

**1. Объекты и субъекты КИИ.**

**2. Структура системы безопасности значимых объектов КИИ.**

Зав. кафедрой ИБ \_\_\_\_\_ И.Г. Сидоркина

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

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

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**

По дисциплине: «Организация защиты объектов критической информационной структуры»

**1. Объекты и субъекты КИИ.**

**2. Структура системы безопасности значимых объектов КИИ.**

Зав. кафедрой ИБ \_\_\_\_\_ И.Г. Сидоркина

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

## Перечень вопросов для проведения промежуточной аттестации

### Перечень

#### вопросов к экзамену

1. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.
2. Объекты и субъекты КИИ.
3. Определение принадлежности к субъектам КИИ, их права и обязанности.
4. Правила категорирования объектов КИИ. Общий порядок работ, сроки категорирования.
5. Критерии значимости объектов КИИ.
6. Создание комиссии по категорированию объектов КИИ. Подготовка исходных данных для категорирования объектов КИИ.
7. Формирование перечня критических процессов.
8. Формирование перечня объектов КИИ, подлежащих категорированию.
9. Оформление и передача в ФСТЭК России результатов категорирования.
10. Внесение изменений в результаты категорирования.
11. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.
12. Особенности обеспечения безопасности объектов КИИ.
13. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
14. Государственный контроль в области обеспечения безопасности объектов КИИ.
15. Цели государственного контроля в области обеспечения безопасности объектов КИИ. 16. Виды и периодичность осуществления контроля объектов КИИ.
17. Реестр значимых объектов КИИ. Цель ведения реестра.
18. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.
19. Перечень показателей критериев значимых объектов КИИ и их значения.
20. Оценка в соответствии с перечнем показателей критериев значимых объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов.
21. Присвоение объектам КИИ одной из категорий значимости либо принятие решения об отсутствии

необходимости присвоения им одной из категорий значимости.

22. Подготовка необходимых документов в рамках категорирования объектов КИИ

23. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ

24. Основные требования по обеспечению безопасности значимых объектов КИИ.

25. Определение вида и типа программных и программно-аппаратных средств защиты информации значимых объектов КИИ.

26. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимых объектов КИИ. Цели и задачи планирования.

27. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности значимых объектов КИИ.

28. Реагирование на компьютерные инциденты в ходе эксплуатации значимых объектов КИИ.

29. Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации.

30. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ.

31. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности для различных категорий значимости объектов КИИ.

32. Цели и задачи системы безопасности значимого объекта КИИ.

33. Требования к созданию систем безопасности значимых объектов КИИ.

34. Требования к силам обеспечения безопасности значимых объектов КИИ.

35. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ.

36. Структура системы безопасности значимых объектов КИИ.

37. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ и обеспечения их функционирования.

38. Оценка соответствия значимых объектов КИИ требованиям по безопасности.

39. Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ и эффективности, принимаемых организационных и технических мер.

40. Юридическая ответственность за нарушения обеспечения безопасности значимых объектов КИИ (уголовная, административная, дисциплинарная).