ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Кафедра «Информатика и информационная безопасность»

РАБОЧАЯ ПРОГРАММА
дисциплины
Б1.В.4 «РАЗРАБОТКА ПРОЕКТНЫХ РЕШЕНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

для специальности
10.05.03 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

по специализации
«*Безопасность автоматизированных систем на железнодорожном транспорте*»

Форма обучения – очная

Санкт-Петербург
2025

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и утверждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 10 от 31 марта 2025 г.

И.о. заведующего кафедрой
«Информатика и информационная безопасность»
31 марта 2025 г. К.З. Билятдинов

СОГЛАСОВАНО

Руководитель ОПОП
31 марта 2025 г. М.Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*Разработка проектных решений по защите информации в автоматизированных системах» Б1.В.04* (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности *10.05.03 «Информационная безопасность автоматизированных систем*» (далее – ФГОС ВО), утвержденного 26 ноября 2020 г., приказ Министерства науки и высшего образования Российской Федерации № 1457, с учетом профессионального стандарта *06.033 «Специалист по защите информации в автоматизированных системах»,* утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н.

Целью изучения дисциплины является формирование у обучающихся способности разрабатывать программные и программно-аппаратные средства для систем защиты информации (СЗИ) автоматизированных систем (АС), проектные решения по защите информации (ЗИ) в АС, включая эксплуатационную документацию на СЗИ АС.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний о:
  - принципах организации и структуре систем защиты информации программного обеспечения автоматизированных систем;
  - методах, способах, средствах, последовательности и содержании этапов разработки АС и СЗИ в АС;
  - основных средствах, способах и принципах построения СЗИ АС;
  - принципах организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения;
- формирование у обучающихся умений:
  - определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в АС;
  - определять структуру СЗИ АС в соответствии с требованиями нормативных правовых документов в области защиты информации;
  - проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов;
  - исследовать эффективность проектных решений программно-аппаратных средств обеспечения ЗИ в АС с целью обеспечения требуемого уровня защищенности;
- формирование у обучающихся навыков:
  - анализа технической документации информационной инфраструктуры автоматизированной системы;
  - документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации;
  - обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
  - синтеза структурных и функциональных схем защищенных автоматизированных систем.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Планируемыми результатами обучения по дисциплине является формирование у обучающихся компетенций и/или части компетенций. Сформированность компетенций и/или части компетенций оценивается с помощью индикаторов достижения компетенций.

В рамках изучения дисциплины осуществляется практическая подготовка обучающихся к будущей профессиональной деятельности. Результатом обучения по дисциплине является формирования у обучающихся практических навыков:

- анализа технической документации информационной инфраструктуры автоматизированной системы;
- документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации;
- обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
- синтеза структурных и функциональных схем защищенных автоматизированных систем.

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ПК-2. Разработка проектных решений по защите информации в автоматизированных системах	
ПК-2.1.4. Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем	Обучающийся *знает*: – стандарты ИБ, применяемые при создании структуры систем ЗИ АС; – подсистемы системы, образующие структуру системы ЗИ АС
ПК-2.2.4. Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах	Обучающийся *умеет*: – составлять техническое задание на создание системы ЗИ АС; – планировать применение системы ЗИ в АС
ПК-2.2.6. Умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Обучающийся *умеет*: – формировать требования к структуре системы ЗИ в АС; – выделять подсистемы в структуре системы ЗИ АС
ПК-3. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	
ПК-3.1.3. Знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах	Обучающийся *знает*: – требования руководящих документов к последовательности и этапности разработки АС и систем ЗИ в АС; – технические, организационные, юридические аспекты интеграция системы ЗИ и АС

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ПК-3.1.4. Знает основные средства, способы и принципы построения систем защиты информации автоматизированных систем	Обучающийся *знает*: – основные способы построения систем ЗИ для АС на железнодорожном транспорте; – способы защиты распределённых АС
ПК-3.2.1. Умеет проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	Обучающийся *умеет*: – категорировать защищаемую АС согласно требованиям руководящих документов; – применять действующие стандарты для проектирования подсистемы безопасности информации АС
ПК-3.2.6. Умеет исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности	Обучающийся *умеет*: – определять требуемый уровень защищённости АС согласно требованиям руководящих документов; – определять вклад каждого элемента ЗИ в общий уровень защищённости АС
ПК-3.3.1. Имеет навыки анализа технической документации информационной инфраструктуры автоматизированной системы	Обучающийся *имеет навык*: – определения наиболее уязвимых мест АС по технической документации на АС; – оценивания целесообразности применения средств ЗИ по технической документации на АС и средства ЗИ
ПК-3.3.4. Имеет навыки документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	Обучающийся *имеет навык*: – подготовки проектной и эксплуатационной документации на инфраструктуру открытых ключей АС ОАО «РЖД»
ПК-3.3.5. Имеет навыки обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	Обучающийся *имеет навык*: – выбора подходящего критерия оценивания эффективности подсистемы обеспечения конфиденциальности; – выбора подходящего критерия оценивания эффективности подсистемы обеспечения доступности; – выбора подходящего критерия оценивания эффективности подсистемы обеспечения целостности
ПК-4. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	
ПК-4.1.4. Знает принципы организации документирования	Обучающийся *знает*: – основные технические решения, применяемые для ЗИ в АС;

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
разработки и процесса сопровождения программного и аппаратного обеспечения	– требования к конструкторской и эксплуатационной документации на подсистему обеспечения конфиденциальности; – требования к конструкторской и эксплуатационной документации на подсистему обеспечения доступности; – требования к конструкторской и эксплуатационной документации на подсистему обеспечения целостности; – особенности документирования системы фиксации и расследования инцидентов информационной безопасности
ПК-4.3.2. Имеет навыки синтеза структурных и функциональных схем защищенных автоматизированных систем	Обучающийся *имеет навык*: – формировать защищаемый периметр АС; – создавать демилитаризованную зону в АС

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений, блока 1 «Дисциплины (модули)».

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Модуль	
		9	А
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	 64 - 128	 32 - 64	 32 - 64
Самостоятельная работа (СРС) (всего)	128	48	80
Контроль	40	36	4
Форма контроля (промежуточной аттестации)		Э	З, КР
Общая трудоемкость: час / з.е.	360/10	180/5	180/5

Примечание: «Форма контроля» – экзамен (Э), зачет (З), зачет с оценкой (З), курсовой проект (КП), курсовая работа (КР)*

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
Семестр 9			
1	Планирование защиты информации в	Лекция 1. Постановка задачи проектирования СЗИ в АС	ПК-2.1.4, ПК-3.1.3,

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
	автоматизированной системе	Лекция 2. Выбор стандартов информационной безопасности и категорирование защищаемой системы	ПК-3.1.4
		Лекция 3. Этапы разработки АС и СЗИ АС	
		Лекция 4. Методы проектирования СЗИ	
		Лабораторная работа 1. Выбор стандартов и категорирование объекта информатизации (ОИ) (4 часа)	
		Лабораторная работа 2. Составление плана разработки СЗИ для АС (4 часа)	
		Лабораторная работа 3. Составление технического задания на проектирование системы ЗИ в АС (4 часа)	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4, ПК-2.2.4, ПК-2.2.6, ПК-3.2.1, ПК-3.2.6, ПК-3.3.1, ПК-3.3.4, ПК-3.3.5
		Лабораторная работа 4. Обоснование затрат на информационную безопасность (4 часа)	
		Самостоятельная работа: – изучение источников [1-2, 6-11]; – изучение нормативных документов [11-12, 18, 21]; подготовка к лабораторным работам [8-10].	
2	Разработка системы ЗИ в АС	Лекция 5. Создание концепции проектирования СЗИ в АС	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4
		Лекция 6. Типы защищаемых данных и способы их защиты	
		Лекция 7. Активы и модель нарушителя	
		Лекция 8. Проектирование контролируемого периметра	
		Лекция 9. Подсистема обеспечения доступности в АС (8 часов)	
		Лекция 10. Подсистема обеспечения целостности в АС (8 часов)	
		Лабораторная работа 5. Разработка структуры СЗИ объекта информатизации (8 часов)	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4, ПК-2.2.4, ПК-2.2.6, ПК-3.2.1, ПК-3.2.6, ПК-3.3.1, ПК-3.3.4, ПК-3.3.5
		Лабораторная работа 6. Описание защищаемого объекта информатизации (4 часа)	
		Лабораторная работа 7. Создание контролируемого периметра (4 часа)	
		Лабораторная работа 8. Обеспечение доступности в распределённых АС (4 часа)	
		Лабораторная работа 9. Проектирование и развёртывание PKI (8 часов)	
		Лабораторная работа 10. Настройка OpenVPN (12 часов)	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Самостоятельная работа: – изучение источников [3-4, 14-17, 19-23]; – подготовка к выполнению лабораторных работ [8-10]	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
Семестр А			
2	Разработка системы ЗИ в АС	Лекция 11. Подсистема обеспечения конфиденциальности в АС (4 часа)	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4, ПК-4.1.4
		Лекция 12. Подсистема фиксации инцидентов ИБ в АС (6 часов)	
		Лекция 13. Демилитаризованная зона и Honey net	
		Лекция 14. Особенности защиты распределённых систем	
		Лекция 15. Оценка безопасности АС	
		Лекция 16. Программа и методика испытаний системы ЗИ	
		Лекция 17. Оформление документации объекта информатизации	
		Лабораторная работа 11. Проектирование подсистемы обеспечения конфиденциальности в АС (8 часов)	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4, ПК-4.1.4, ПК-2.2.4, ПК-2.2.6, ПК-3.2.1, ПК-3.2.6, ПК-3.3.1, ПК-3.3.4, ПК-3.3.5, ПК-4.3.2
		Лабораторная работа 12. Создание подсистемы фиксации и расследования инцидентов (8 часов)	
		Лабораторная работа 13. Создание демилитаризованной зоны в АС (4 часа)	
		Лабораторная работа 14. Описание рисков информационной системы (4 часа)	
		Лабораторная работа 15. Исследование эффективности возможных проектных решений СЗИ (4 часа)	
		Лабораторная работа 16. Синтез структурных и функциональных схем защищенных автоматизированных систем (4 часа)	
		Лабораторная работа 17. Организация электронного документооборота в системе ЗИ АС (4 часа)	
		Самостоятельная работа: – изучение источников [3-4, 14-17, 19-23]; – подготовка к выполнению лабораторных работ [8-10]. Курсовая работа	
3	Сдача в эксплуатацию системы ЗИ	Лекция 18. Технические, организационные, юридические аспекты интеграция СЗИ и АС	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4,
		Лекция 19. Способы внедрения СЗИ в АС	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лекция 20. Сопротивление внедрению СЗИ	ПК-4.1.4
		Лекция 21. Опытная и промышленная эксплуатация СЗИ, сопровождение и обновление СЗИ	
		Лекция 22. Особенности работы с регуляторами (4 часа)	
		Лекция 23. Заключение. Изъятие из эксплуатации и утилизация СЗИ	
		Лабораторная работа 18 Интеграция системы ЗИ и АС (8 часов)	ПК-2.1.4, ПК-3.1.3, ПК-3.1.4, ПК-4.1.4, ПК-2.2.4, ПК-2.2.6, ПК-3.2.1, ПК-3.2.6, ПК-3.3.1, ПК-3.3.4, ПК-3.3.5, ПК-4.3.2
		Лабораторная работа 19. Разработка документации для СЗИ (8 часов)	
		Лабораторная работа 20. Требования регуляторов к информационным системам РЖД	
		Лабораторная работа 21. Исследование корреляций понятий информационной безопасности	
		Самостоятельная работа: – изучение источников [5, 7, 11-23]; – подготовка к выполнению лабораторных работ [8-10]. Курсовая работа	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
Семестр 9						
1	Планирование защиты информации в автоматизированной системе	8	0	16	16	40
2	Разработка системы ЗИ в АС	24	0	48	32	104
	Итого	32	0	64	48	144
					Контроль	
					Всего (общая трудоемкость, час.)	180
Семестр А						
2	Разработка системы ЗИ в АС	18	0	36	40	104
2	Разработка системы ЗИ в АС	14	0	22	40	40
	Итого	32	0	64	80	144
					Контроль	36
					Всего (общая трудоемкость, час.)	180

6. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценочные материалы по дисциплине является неотъемлемой частью рабочей программы и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

7. Методические указания для обучающихся по освоению дисциплины

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины, используя методические материалы дисциплины, а также учебно-методическое обеспечение, приведенное в разделе 8 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем успеваемости (см. оценочные материалы по дисциплине).
3. По итогам текущего контроля успеваемости по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. оценочные материалы по дисциплине).

8. Описание материально-технического и учебно-методического обеспечения, необходимого для реализации образовательной программы по дисциплине

8.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, укомплектованные специализированной учебной мебелью и оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории: настенным экраном (стационарным или переносным), маркерной доской и (или) меловой доской, мультимедийным проектором (стационарным или переносным).

Все помещения, используемые для проведения учебных занятий и самостоятельной работы, соответствуют действующим санитарным и противопожарным нормам и правилам.

Для проведения лабораторных работ используется лаборатория программно-аппаратных средств обеспечения информационной безопасности, оборудованная компьютерной техникой с установленными программными средствами обеспечения информационной безопасности и виртуализации, перечисленными в п. 8.2.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

8.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- MS Office;
- Операционная система Windows;
- Антивирус Касперский;
- VMware workstation или VirtualBox.

8.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных:

- Электронно-библиотечная система издательства «Лань». [Электронный ресурс]. – URL: https://e.lanbook.com/ — Режим доступа: для авториз. пользователей;
- Электронно-библиотечная система ibooks.ru («Айбукс»). – URL: https:// ibooks.ru / — Режим доступа: для авториз. пользователей;
- Электронная библиотека ЮРАЙТ. – URL: https://biblio-online.ru/ — Режим доступа: для авториз. пользователей;

– Единое окно доступа к образовательным ресурсам - каталог образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования». – URL: http://window.edu.ru/ — Режим доступа: свободный.

– Словари и энциклопедии. – URL: http://academic.ru/ — Режим доступа: свободный.

– Научная электронная библиотека "КиберЛенинка" – URL: http://cyberleninka.ru/ — Режим доступа: свободный.

8.4. Обучающимся обеспечен доступ (удаленный доступ) к информационным справочным системам:

– Национальный Открытый Университет "ИНТУИТ". Бесплатное образование. [Электронный ресурс]. – URL: https://intuit.ru/ — Режим доступа: свободный.

– Техническая документация по языку программирования Python [Электронный ресурс] – Режим доступа: https://www.python.org/doc/ (свободный доступ).

– Техническая документация по языку программирования и платформе Java [Электронный ресурс] – Режим доступа: https://docs.oracle.com/en/java/ (свободный доступ).

8.5. Перечень печатных и электронных изданий, используемых в образовательном процессе:

1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 440 с.

2. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 448 с.

3. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с.

4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. - М.: Горячая линия–Телеком, 2014. - 244 с.

5. Грызунов В.В. Абсолютный мотиватор (учебное пособие). – М: ЛитРес:Самиздат, 2020 – 109с.

6. Расторгуев С.П. Информационная война. — М: Радио и связь, 1999. — 416 С. — ISBN 5-256-01399-8 https://vk.com/doc-135429705_462253189.

7. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие - М.: Горячая линия - Телеком, 2012. - 214с.

8. П.Ю. Богданов, В.В. Грызунов, Е.П. Истомин, Т.М. Татарникова, Н.В. Яготинцева. Методы защиты информации. Учебное пособие. - СПб.: ООО «Андреевский издательский дом», 2019 - 74 с

9. В.Г. Бурлов, В.В. Грызунов. IT-инструменты для обработки, представления и передачи данных в исследовательской работе (учебное пособие).- СПб.: ООО «Андреевский издательский дом», 2018.- 96с.

10. В.В. Грызунов, Н.В. Яготинцева. Защита операционных систем (учебное пособие).- СПб.: ООО «Андреевский издательский дом», 2018.- 172с.

11. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

12. Федеральные законы:

• «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006;

- «О коммерческой тайне» № 119-ФЗ от 29.07.2004;
- «О персональных данных» № 152-ФЗ от 27.07.2006.

13. Сборник Руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа – М: Гостехкомиссия, 1998. – 120 с.

14. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

15. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3.

16. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

17. ГОСТ ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

18. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении.

19. ГОСТ 2.102-2013. Виды и комплектность конструкторских документов

20. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.- М.: Стандартинформ, 2012. -12 с.

21. СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения» // ОАО «РЖД», 2009.

22. Основные положения защиты информационной инфраструктуры ОАО «РЖД» // ОАО «РЖД», 2013.

23. Политика информационной безопасности ОАО «РЖД // ОАО «РЖД», 2013.

8.6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых в образовательном процессе:

– Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://my.pgups.ru — Режим доступа: для авториз. пользователей;

– Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://sdo.pgups.ru — Режим доступа: для авториз. пользователей;

– Электронный фонд правовой и нормативно-технической документации – URL: http://docs.cntd.ru/ — Режим доступа: свободный.

В.В. Грызунов

Разработчик рабочей программы, *доцент*
31 марта 2025 г.