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.О.41 «ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ И ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ»
для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на транспорте*»

Форма обучения – очная

Санкт-Петербург
2026

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и утверждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 6 от 28 января 2026 г.

И.о. заведующего кафедрой
«Информатика и информационная безопасность»
28 января 2026 г. К.З. Билятдинов

СОГЛАСОВАНО

Руководитель ОПОП
28 января 2026 г. М.Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ И ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ» (Б1.О.41*) (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 расширение и углубление профессиональной подготовки для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности и специализацией «Информационная безопасность автоматизированных систем на транспорте»

Для достижения цели дисциплины решаются следующие задачи:

- изучение методологии проведения комплексного анализа защищенности и инструментального мониторинга распределенных информационных систем;
- изучение принципов проектирования и оценивания надежности результатов разработки программных элементов распределенных информационных систем;
- анализ возможностей эксплуатации распределенных информационных систем с учетом специфики угроз информации в них.

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.

- ОПК-9.3.3. Имеет навыки имеет навыки проектирования распределенных информационных систем, в том числе разработки приложений, реализующих параллельные вычисления

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	
ОПК-9.1.4. Знает особенности построения, функционирования и защиты современных центров обработки данных, распределенных информационных систем и их коммуникационной	*Обучающийся знает:* построения, функционирования и защиты современных центров обработки данных, распределенных информационных систем и их коммуникационной среды

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
среды	
ОПК-9.2.3. Умеет определять требования по защите коммуникационной среды распределенной информационной системы	*Обучающийся умеет:* определять требования по защите и проводить комплексный анализ защищенности и инструментальный мониторинг распределенных информационных систем
ОПК-9.3.3. Имеет навыки проектирования распределенных информационных систем, в том числе разработки приложений, реализующих параллельные вычисления	*Обучающийся владеет* основными методами проектирования программных элементов распределенных информационных систем

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)». (*обязательная часть)*

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		9
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	96 32 64	96 32 64
Самостоятельная работа (СРС) (всего)	48	48
Контроль	36	36
Форма контроля (промежуточной аттестации)	Э	Э
Общая трудоемкость: час / з.е.	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
1	Защита информации в распределенных информационных системах	Лекция 1.1 Задачи и требования к распределенной информационной системе	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лекция 1.2 Аппаратные решения распределенной информационной системы	ОПК-9.1.5. ОПК-9.3.3.
		Лекция 1.3 Программные решения распределенной информационной	ОПК-9.1.5. ОПК-9.3.3.

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		системы	
		Лекция 1.4 Эволюция распределенных вычислений и систем	ОПК-9.1.5. ОПК-9.3.3.
		Лекция 1.5 Распределенные информационные системы на транспорте.	ОПК-9.1.5. ОПК-9.3.3.
		Лекция 1.6 Особенности защиты информации в распределенных информационных системах	ОПК-9.2.3. ОПК-9.3.3.
		Лабораторная работа №1 «Построение приложения, реализующего концепцию многозадачности и распределенных вычислений» (16 час)	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Литература: [1] – [3] Интернет-ресурсы [1] – [6]	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
2	Безопасность коммуникационной среды распределенных информационных систем	Лекция 2.1 Характеристика мультисервисной телекоммуникационной сети ОАО «РЖД»	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лекция 2.2 Информационная безопасность ЕМЦСС	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лекция 2.3 Система передачи данных ОАО «РЖД»	ОПК-9.1.5. ОПК-9.3.3.
		Лекция 2.4 Система обеспечения информационной безопасности СПД ОАО «РЖД»	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лекция 2.5 Обеспечение информационной безопасности системы цифровой технологической радиосвязи стандарта GSM-R	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лекция 2.6 Беспроводные технологии и сети радиодоступа	ОПК-9.2.3. ОПК-9.3.3.
		Лекция 2.7 Защита информации в беспроводных сетях радиодоступа	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лабораторная работа №2 «Проектирование распределенной информационной системы» (16 час)	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Лабораторная работа №3 «Создание распределенной информационной системы в защищенном исполнении» (32 час)	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения.	ОПК-9.1.5. ОПК-9.2.3. ОПК-9.3.3.

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Литература: [3] - [11] Интернет-ресурсы [1] – [6]	
3	Информационная безопасность центров обработки данных	Лекция 3.1 Центры обработки данных. Серверный комплекс. Система хранения данных.	ОПК-9.1.6.
		Лекция 3.2 Резервный центр. Система резервного копирования. «Обеспечивающая» инженерная инфраструктура.	ОПК-9.1.6.
		Лекция 3.3 Системы управления и мониторинга. Стандарты управления ЦОД.	ОПК-9.1.6.
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Литература: [3] - [11] Интернет-ресурсы [1] – [6]	ОПК-9.1.6.

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Защита информации в распределенных информационных системах	12		16	16	44
2	Информационная безопасность центров обработки данных	14		48	24	86
3	Безопасность коммуникационной среды распределенных информационных систем	6			8	14
	Итого	32		64	48	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, 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 кафедры «*Лаборатория защищенных автоматизированных систем»* оборудованная следующими приборами/специальной техникой/установками используемыми в учебном процессе:

– Visual Studio C/C++

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:

Перечень лицензионных программ представлен на внутреннем портале ФГБОУ ВО ПГУПС по адресу http://eaisu.pgups.edu.mps/info/prog/

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" - это научная электронная библиотека, построенная на парадигме открытой науки (Open Science), основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии и повышение цитируемости российской науки. – 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.

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

1. Защита информации безопасность в распределенных информационных системах. / А.А. Корниенко, А.П. Глухов, С.В. Диасамидзе. - СПб: ФГБОУ ВО ПГУПС, 2018. – 41 с.

2. Варфоломеев, В.А. Высокопроизводительные вычислительные системы на железнодорожном транспорте. [Электронный ресурс] / В.А. Варфоломеев, Э.К. Лецкий, М.Н. Шамров, В.В. Яковлев. — Электрон. дан. — М. : УМЦ ЖДТ, 2010. — 246 с. — Режим доступа: http://e.lanbook.com/book/4163

3. 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.

4. Корниенко А.А., Поляничко М.А. Стандарты информационной безопасности (учебное пособие). – СПб.: ПГУПС, 2011. – 72 с.

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

Перечень нормативно-правовой документации, необходимой для освоения дисциплины

6. 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.

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

8. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: ИПК Издательство стандартов, 2008.

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

10. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

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

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

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

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

3. Официальный портал Росстандарта http://www.gost.ru/wps/portal/, портал по стандартизации http://standard.gost.ru/wps/portal/

4. Официальный сайт ФСТЭК России http://www.fstec.ru/

5. Проект «Информационная безопасность». http://www.itsec.ru/

6. Проект «Национальный Открытый Университет «ИНТУИТ» http://www.intuit.ru/

Разработчик рабочей программы, проф. А.А. Корниенко
23.01.2026