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.42 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ТРАНСПОРТЕ»
для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на 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 «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ТРАНСПОРТЕ»» (Б1.О.42*) (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 автоматизированных транспортных систем;
- изучение принципов проектирования и оценивания надежности результатов разработки программных элементов автоматизированных транспортных систем;
- изучение методологии проектирования и оценивания эффективности системы защиты информации автоматизированных на транспорте;
- анализ возможностей эксплуатации программно-аппаратных средств защиты автоматизированных транспортных 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-9.1.3.1. Имеет навыки применения методов и средств защиты информации при построении систем защиты информации автоматизированных на транспорте
- ОПК-9.3.3.1. Имеет навыки применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте

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-9.1.1.1. Знает особенности проектирования систем защиты	*Обучающийся знает* принципы проектирования автоматизированных

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте	транспортных систем
ОПК-9.2.1.1. Знает особенности эксплуатации систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте	*Обучающийся знает:* особенности эксплуатации программно-аппаратных средств защиты автоматизированных транспортных систем с учетом специфики угроз информации в них
ОПК-9.3.1.1. Знает основные угрозы и уязвимости, методы контроля защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте с учетом установленных требований	*Обучающийся знает:* основные угрозы и уязвимости, методы контроля защищенности автоматизированных транспортных систем
ОПК-9.1.2.1. Умеет проектировать систему защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами на транспорте	*Обучающийся умеет:* проектировать систему защиты информации автоматизированных транспортных систем
ОПК-9.2.2.1. Умеет осуществлять внедрение систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	*Обучающийся умеет:* выбрать и внедрить средства защиты информации автоматизированных транспортных систем
ОПК-9.3.2.1. Умеет выявлять уязвимости прогнозировать и устранять угрозы информационной безопасности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе в автоматизированных систем управления технологическими процессами, в течение всего времени их применения	*Обучающийся умеет* выявлять и устранять основные угрозы и уязвимости автоматизированных транспортных систем
ОПК-9.1.3.1. Имеет навыки применения методов и средств защиты информации при построении систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	*Обучающийся имеет навыки применения* основных методов защиты информации автоматизированных транспортных систем

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК-9.2.3.1. Владеет методами эксплуатации систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся владеет принципами эксплуатации систем защиты информации автоматизированных систем на транспорте
ОПК-9.3.3.1. Имеет навыки применения автоматизированных средств контроля защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся имеет навыки применения средств контроля защищенности автоматизированных систем на транспорте

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)	80 32 48	80 32 48
Самостоятельная работа (СРС) (всего)	60	60
Контроль	4	4
Форма контроля (промежуточной аттестации)	З, КП	З, КП
Общая трудоемкость: час / з.е.	144 / 4	144 / 4

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	Характеристика автоматизированных систем ОАО «РЖД» как объектов систем информационной	Лекция 1.1 Общая характеристика автоматизированных систем ОАО «РЖД»	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Лекция 1.2 Автоматизированные системы управления ресурсами предприятия (ERP-системы) на примере ЕК АСУФР	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
	безопасности	Лекция 1.3 Автоматизированная система ЭТРАН	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Лекция 1.4 АСУ «Экспресс-3» как распределенная информационная система	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Лекция 1.5 Автоматизированные системы управления перевозками	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Лекция 1.6 Система ГИД «Урал-ВНИИЖТ»	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Лабораторная работа №1 «Изучение систем требований в области защиты информации и информационной безопасности» (16 час)	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Выполнение курсового проекта. Подготовка к защите курсового проекта. Подготовка к сдаче зачета). Литература: [1], [6] Интернет-ресурсы [1] – [6]	ОПК-9.1.1.1 ОПК-9.2.1.1 ОПК-9.3.1.1
2	Информационная безопасность критической информационной инфраструктуры	Лекция 2.1 Характеристика ERP-систем российских железных дорог как объектов информационной безопасности (4 час)	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.2 Система обеспечения информационной безопасности АСУ «Экспресс-3»	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.3 Автоматизированная система ЭТРАН как объект информационной безопасности	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
			ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.4 Основные сервисы безопасности и методы защиты информации в корпоративных информационных системах и сетях (6 час)	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.5 Корпоративные политики информатизации и информационной безопасности	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.6 Система оценки защищенности автоматизированных информационных и телекоммуникационных систем ОАО «РЖД»	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лекция 2.7 Система обнаружения, предупреждения и ликвидации последствий компьютерных атак	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лабораторная работа №2 «Классификация корпоративной автоматизированной системы или сети по требованиям безопасности информации» (8 час)	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Лабораторная работа №3 «Разработка	ОПК-9.1.1.1

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		примерного профиля защиты для ERP-системы» (24 час)	ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Выполнение курсового проекта. Подготовка к защите курсового проекта. Подготовка к сдаче зачета). Литература: [1] - [12] Интернет-ресурсы [1] – [6]	ОПК-9.1.1.1 ОПК-9.1.2.1 ОПК-9.1.3.1 ОПК-9.2.1.1 ОПК-9.2.2.1 ОПК-9.2.3.1 ОПК-9.3.1.1 ОПК-9.3.2.1 ОПК-9.3.2.3 ОПК-9.3.3.1

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Характеристика автоматизированных систем ОАО «РЖД» как объектов систем информационной безопасности	12		16	20	48
2	Методы и средства обеспечения информационной безопасности автоматизированных систем	20		32	40	92
	Итого	32		48	60	140
					Контроль	4
					Всего (общая трудоемкость, час.)	144

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 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:

– MS Office;
– Операционная система Windows;
– Антивирус Касперский;
– Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ».

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. Информационная безопасность и защита информации на железнодорожном транспорте. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. — М. : УМЦ ЖДТ, 2014. — 440 с.
2. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 448 с.
3. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2016. – 45 с.
4. Профили защиты и задания по безопасности корпоративных информационных систем и сетей железнодорожного транспорта: учебное пособие. – СПб: ПГУПС, 2014. – 94 с.
5. Кибербезопасность и защита от компьютерных атак на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2015. – 50 с.
6. Корпоративные информационные системы на железнодорожном транспорте. [Электронный ресурс] — Электрон. дан. — М. : УМЦ ЖДТ, 2013. — 256 с. — Режим доступа: http://e.lanbook.com/book/60017

Перечень нормативно-правовой документации, необходимой для освоения дисциплины

7. 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.
8. Сборник Руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа – М: Гостехкомиссия, 1998. – 120 с.
9. 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.
10. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
11. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
12. 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
31.03.2025