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.43 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ И ИНФОРМАЦИОННО-ЛОГИСТИЧЕСКИХ СИСТЕМ НА ТРАНСПОРТЕ»

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 «*Информационная безопасность информационно-управляющих и информационно-логистических систем на транспорте» (Б1.О.43*) (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 осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на железнодорожном транспорте (ИУиИЛС), в том числе автоматизированных систем управления технологическими процессами (АСУ ТП), а так же проектировать системы защиты информации ИУиИЛС и АСУ ТП, сопровождать их разработку.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний об особенностях ИУиИЛС и АСУ ТП в части:
    - существующих угроз и уязвимостей, методов контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте
    - эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте
    - проектирования систем защиты информации ИУиИЛС и АСУ ТП;
- формирование у обучающихся умений при работе с ИУиИЛС и АСУ ТП:
    - анализировать, прогнозировать и устранять угрозы информационной безопасности;
    - выявлять уязвимости;
    - проектировать систему защиты информации;
    - осуществлять внедрение систем защиты информации;
- формирование у обучающихся навыков при работе с ИУиИЛС и АСУ ТП:
    - применения методов и средств защиты информации при построении систем защиты информации;
    - эксплуатировать системы защиты информации;
    - применения автоматизированных средств контроля защищенности.

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 применения в интересах ИУиИЛС и АСУ ТП:

- методов и средств защиты информации;
- автоматизированных средств контроля защищенности.

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК-9.1. Способен проектировать системы защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на железнодорожном транспорте и сопровождать их разработку	
ОПК-9.1.1.2. Знает особенности проектирования систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте	Обучающийся *знает*: – особенности АСУ ТП и ИУиИЛС на транспорте с точки зрения проектирования систем защиты информации; – способы проектирования систем защиты информации для АСУ ТП и ИУиИЛС на транспорте
ОПК-9.1.2.2. Умеет проектировать систему защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся *умеет*: – предъявлять требования к системе защиты информации АСУ ТП и ИУиИЛС на транспорте при проектировании; – выбирать структуру системы защиты информации АСУ ТП и ИУиИЛС на транспорте
ОПК-9.1.3.2. Имеет навыки применения методов и средств защиты информации при построении систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся *имеет навыки*: – выполнения резервного копирования критической информации АСУ ТП и ИУиИЛС на транспорте; – защиты распределённых вычислений в АСУ ТП и ИУиИЛС на транспорте.
ОПК-9.2. Способен осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на железнодорожном транспорте	
ОПК-9.2.1.2. Знает особенности эксплуатации систем защиты информации информационно-управляющих и информационно-	Обучающийся *знает*: – методы и средства администрирования систем защиты информации в MS Windows и Linux; – модели нарушителя АСУ ТП и ИУиИЛС на транспорте; – особенности защиты мобильных пользователей АСУ

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
логистических систем на транспорте	ТП и ИУиИЛС на транспорте
ОПК-9.2.2.2. Умеет осуществлять внедрение систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся *умеет*: – внедрять и настраивать политики безопасности для MS Windows, Linux; – рассчитывать время жизни средства защиты информации АСУ ТП и ИУиИЛС на транспорте.
ОПК-9.2.3.2. Владеет методами эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся *имеет навык* защиты в АСУ ТП и ИУиИЛС на транспорте: – информации путём резервного копирования; – облачных решений; – базы данных
ОПК-9.3. Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на железнодорожном транспорте с учетом установленных требований безопасности	
ОПК-9.3.1.2. Знает основные угрозы и уязвимости, методы контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте	Обучающийся *знает* для АСУ ТП и ИУиИЛС на транспорте: – основные угрозы и уязвимости, а также методы их обнаружения; – языки описания угроз и уязвимостей; – уязвимости аппаратной части; – уязвимости уровня персонала
ОПК-9.3.2.2. Умеет выявлять уязвимости в информационно-управляющих и информационно-логистических системах на транспорте, в том числе в автоматизированных системах управления технологическими процессами	Обучающийся *умеет* выявлять и описывать уязвимости АСУ ТП и ИУиИЛС на транспорте: – на программном уровне; – на аппаратном уровне; – на уровне персонала

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК-9.3.2.4. Умеет анализировать, прогнозировать и устранять угрозы информационной безопасности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами, в течение всего времени их применения	Обучающийся *умеет*: – прогнозировать действия нарушителя информационно безопасности АСУ ТП и ИУиИЛС на транспорте; – подбирать и настраивать средства защиты информации, нейтрализующие выявленные угрозы информационной безопасности
ОПК-9.3.3.2. Имеет навыки применения автоматизированных средств контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами	Обучающийся *имеет навыки*: – применять автоматизированные средства контроля защищённости облачных АСУ ТП и ИУиИЛС на транспорте; – контролировать с помощью автоматизированных средств защищённость распределённых АСУ ТП и ИУиИЛС на транспорте

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части блока 1 «Дисциплины (модули)».

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	 32 - 32
Самостоятельная работа (СРС) (всего)	40
Контроль	4
Форма контроля (промежуточной аттестации)	
Общая трудоемкость: час / з.е.	108/3

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
9 семестр			
1	Уязвимости АСУ ТП и ИУиИЛС на транспорте	Лекция 1. АСУ ТП и ИУиИЛС на транспорте как объект злоумышленных действий. Уязвимости баз данных в АСУ ТП и ИУиИЛС и способы их устранения	ОПК-9.1.1.2, ОПК-9.2.1.2. ОПК-9.3.1.2.
		Лекция 2. Уязвимости и информационная безопасность при применении средств виртуализации	
		Лекция 3. Уязвимости аппаратной части АСУ ТП и ИУиИЛС и способы их устранения (4 часа)	
		Лекция 4. Уязвимости распределённых АСУ ТП и ИУиИЛС	
		Лекция 5. Языки описания уязвимостей АСУ ТП и информационно-управляющих и информационно-логистических систем на транспорте (4 часа)	
		Лекция 6. Уязвимости на уровне персонала АСУ ТП и ИУиИЛС и способы их устранения	
		Лекция 7. Планирование и реализация информационно-технических вторжений в АСУ ТП и ИУиИЛС на транспорте	ОПК-9.1.1.2, ОПК-9.2.1.2, ОПК-9.3.1.2, ОПК-9.1.2.2, ОПК-9.1.3.2, ОПК-9.2.2.2, ОПК-9.2.3.2, ОПК-9.3.2.2, ОПК-9.3.2.4, ОПК-9.3.3.2
		Лабораторная работа 1. SQL-injection АСУ ТП и ИУиИЛС (4 часа)	
		Лабораторная работа 2. Создание корпоративного облака в ИУиИЛС (4 часа)	
		Лабораторная работа 3. Безопасность распределённых вычислений АСУ ТП и ИУиИЛС (4 часа)	
		Лабораторная работа 4. Описание уязвимостей информационной системы (4 часа)	
		Лабораторная работа 5. Выявление и устранение уязвимостей на уровне персонала АСУ ТП и ИУиИЛС	
		Самостоятельная работа: – изучение части 1 учебника [1], [3]; – изучение нормативных документов; – подготовка к лабораторным работам [3-5].	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
2	Обеспечение безопасности АСУ ТП и ИУиИЛС на транспорте	Лекция 8. Организационно-технические особенности защиты информации в АСУ ТП и ИУиИЛС на транспорте	ОПК-9.1.1.2, ОПК-9.2.1.2, ОПК-9.3.1.2, ОПК-9.1.2.2, ОПК-9.1.3.2, ОПК-9.2.2.2, ОПК-9.2.3.2, ОПК-9.3.2.2, ОПК-9.3.2.4, ОПК-9.3.3.2
		Лекция 9. Модель нарушителя АСУ ТП и информационно-управляющих и информационно-логистических систем на транспорте (4 часа)	
		Лекция 10. Модели безопасности в АСУ ТП и ИУиИЛС (4 часа)	
		Лекция 11. Информационная безопасность мобильных элементов АСУ ТП и ИУиИЛС	
		Лекция 12. АСУ ТП и ИУиИЛС как объект критической информационной инфраструктуры и ГосСОПКА	
		Лабораторная работа 6. Исследование времени жизни средства защиты информации (4 часа)	
		Лабораторная работа 7. Политики безопасности Linux, MS Windows (6 часов)	
		Лабораторная работа 8. Управление резервными копиями (4 часа)	
		Самостоятельная работа: – изучение 2 части учебника [2], [6]; – подготовка к выполнению лабораторных работ [3-5].	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
9 семестр						
1	Уязвимости АСУ ТП и ИУиИЛС на транспорте	20	0	18	24	62
2	Обеспечение безопасности АСУ ТП и ИУиИЛС на транспорте	12	0	14	16	42
	Итого	32	0	32	40	104
					Контроль	4
					Всего (общая трудоемкость, час.)	108

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. А. А. Корниенко, А. П. Глухов, С. В. Диасамидзе. Система предупреждения и обнаружения компьютерных атак (учебное пособие). - СПб.: ПГУПС, 2019. – 47 с.

4. 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

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

6. Надежность систем железнодорожной автоматики, телемеханики и связи: учебное пособие / В. В. Сапожников [и др.] ; ред. В. В. Сапожников. - Москва : Учебно-методический центр по образованию на железнодорожном транспорте, 2017. - 316 с.

7. Нормативные документы:

- Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);
- Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»
- Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
- Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
- Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
- Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»
- Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

- Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»
- 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, *профессор*
19 марта 2025 г.