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.3 «*ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ И СРЕДСТВА КОНТРОЛЯ*»
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 «*Техническая защита информации и средства контроля» (Б1.В.3*) (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 знаний в области тестирования систем защиты информации автоматизированных систем и в области разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний о технических средствах контроля эффективности мер защиты информации;
- формирование у обучающихся навыков разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

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.

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ПК-1 Тестирование систем защиты информации автоматизированных систем	
ПК-1.1.5 Знает технические средства контроля эффективности мер защиты информации	Обучающийся знает: – особенности технической защиты информации; – технические средства контроля эффективности мер защиты информации.
ПК-4 Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	
ПК-4.3.3 Имеет навыки разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	Обучающийся имеет навыки: – разработки программного обеспечения для обеспечения защиты информации; – разработки баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации; – использования технических средств для обеспечения защиты информации.

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

– разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

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	Семестр
		6
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)	28	28
Контроль	36	36
Форма контроля (промежуточной аттестации)	Э	Э
Общая трудоемкость: час / з.е.	144/4	144/4

Примечание: «Форма контроля» – экзамен (Э)

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Источники угрозы безопасности информации.	**Лекция 1.** Вводная лекция. Основные направления защиты информации. Система показателей защищенности (4 часа). **Лекция 2.** Объекты защиты информации. Классификация объектов. Демаскирующие признаки. Источники опасных сигналов. **Лекция 3.** Основные концептуальные положения инженерно-технической защиты информации. Основные проблемы инженерно-технической защиты информации.	ПК-1.1.5 ПК-4.3.3
		Лабораторная работа 1. Анализ генераторов шума. **Лабораторная работа 2.** Исследование работы анализатора и генератора сигналов.	ПК-1.1.5 ПК-4.3.3
		Самостоятельная работа. Изучить главу в учебнике «Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А.	ПК-1.1.5 ПК-4.3.3

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с.» Подготовиться к выполнению лабораторных работ.	
2	Техническое противодействие техническим средствам разведки	**Лекция 4.** Методы и средства добывания информации. Основные задачи и органы технической разведки. **Лекция 5.** Принципы технической разведки. Основные этапы и процессы добывания информации технической разведки. Классификация технической разведки. **Лекция 6.** Средства перехвата информации по техническим каналам утечки информации. Средства обеспечения технической защиты информации. **Лекция 7.** Способы и средства противодействия различным видам разведки.	ПК-1.1.5 ПК-4.3.3
		Лабораторная работа 3. Защита телефонных линий. **Лабораторная работа 4.** Исследование работы портативного обнаружителя полупроводниковых элементов. **Лабораторная работа 5.** Оценка защищенности речевой информации.	ПК-1.1.5 ПК-4.3.3
		Самостоятельная работа. Изучить главу в учебном пособии Меньшаков Ю.К. Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ. ред. М.П. Сычева. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. – 478 с. Подготовиться к выполнению лабораторных работ.	ПК-1.1.5 ПК-4.3.3
3	Пассивные и активные средства защиты информации.	**Лекция 8.** Организационные мероприятия по защите информации. Пассивные средства защиты. **Лекция 9.** Технические мероприятия по защите информации. Активные средства защиты (4 часа).	ПК-1.1.5 ПК-4.3.3
		Лабораторная работа 6. Аналитическое обоснование необходимости создания подсистемы технической защиты объекта	ПК-1.1.5 ПК-4.3.3

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		информатизации.	
		Самостоятельная работа. Изучить учебное пособие Глухарев М.Л., Исаева М.Ф. Технические средства защиты информации: учеб. пособие / М.Л. Глухарев, М.Ф. Исаева. – СПб: ФГБОУ ВО ПГУПС, 2018. – 55 с. Изучить главу в учебнике «Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.» Подготовиться к выполнению лабораторных работ.	ПК-1.1.5 ПК-4.3.3
4	Основы контроля эффективности мер защиты информации	**Лекция 10.** Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. **Лекция 11.** Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. **Лекция 12**. Методы и средства контроля эффективности технической защиты информации.	ПК-1.1.5 ПК-4.3.3
		Лабораторная работа 7. Организация технической защиты информации. **Лабораторная работа 8.** Проверка радиоэфира с использованием радиоприемника AOR AR5000.	ПК-1.1.5 ПК-4.3.3
		Самостоятельная работа. Изучить главу в учебнике «Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.» Подготовиться к выполнению лабораторных работ.	ПК-1.1.5 ПК-4.3.3
5	Правовое и организационное обеспечение информационной безопасности	**Лекция 13.** Основы нормативно-правового обеспечения зашиты информации. **Лекция 14.** Основы организации защиты информации на объектах информатизации. Проведение аттестации выделенных помещений, аттестации объектов информатизации.	ПК-1.1.5 ПК-4.3.3

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лабораторная работа 9. Организация и проведение аттестации объектов информатизации и выделенных помещений. **Лабораторная работа 10.** Основные требования нормативных документов ФСТЭК России по технической защите объектов информатизации и выделенных помещений.	ПК-1.1.5 ПК-4.3.3
		Самостоятельная работа. Изучить главу в учебнике «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. – 439 с.». Изучить законодательство Российской федерации в области технической защиты информации. Подготовиться к выполнению лабораторных работ.	ПК-1.1.5 ПК-4.3.3

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Источники угрозы безопасности информации	8	0	10	5	23
2	Техническое противодействие техническим средствам разведки	8	0	12	6	26
3	Пассивные и активные средства защиты информации	6	0	8	6	20
4	Основы контроля эффективности мер защиты информации	6	0	8	6	20
5	Правовое и организационное обеспечение информационной безопасности	4	0	10	5	19
	Итого	32	-	48	28	108
					Контроль	36
					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.

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" – 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:

– 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. – 439 с.

– 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. – 447 с.

– Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

– Исаева М.Ф. Техническая защита информации / М.Ф. Исаева – СПб: ФГБОУ ВО ПГУПС, 2017. – 48 с.

– Беляков И.А. Технические каналы утечки информации / И.А. Беляков – СПб: ФГБОУ ВО ПГУПС, 2017. – 33 с.

– Глухарев М.Л., Исаева М.Ф. Технические средства защиты информации: учеб. пособие / М.Л. Глухарев, М.Ф. Исаева. – СПб: ФГБОУ ВО ПГУПС, 2018. – 55 с.

– Меньшаков Ю.К.Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ. ред. М.П. Сычева. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2011. – 478 с.

– Федеральный закон «Об электронной подписи» No 63-ФЗ от 06.04.2011;

– ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

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;

– Правовая система КонсультантПлюс. – URL:http://www.consultant.ru/ — Режим доступа: свободный.

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

Разработчик рабочей программы, старший преподаватель М.Ф. Соломатова

16 марта 2025 г.