

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.31 «ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

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 «*Защита информации от утечки по техническим каналам*» (Б1.О.31) (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 решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний о текущем состоянии и тенденции развития методов и средств защиты информации от утечки по техническим каналам;
- формирование у обучающихся знаний о технических каналах утечки информации, об организации защиты информации от утечки по техническим каналам, основных характеристиках и принципах построения средств защиты информации от утечки по техническим каналам;
- формирования у обучающихся умений применять средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности

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)
<i>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</i>	
ОПК-9.1.2. Знает технические каналы утечки информации; организацию, основные характеристики и принципы построения средств защиты информации от утечки по техническим каналам; текущее состояние и тенденции развития методов и средств защиты информации от утечки по техническим каналам	Обучающийся знает: – технические каналы утечки информации; – организацию, основные характеристики и принципы построения средств защиты информации от утечки по техническим каналам – текущее состояние и тенденции развития методов и средств защиты информации от утечки по техническим каналам
ОПК-9.2.2. Умеет применять средства защиты от утечки по	Обучающийся умеет: – выбирать и применять необходимые средства

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
техническим каналам при решении задач профессиональной деятельности	защиты информации от её утечки по техническим каналам; – решать задачи по обеспечению защиты информации от утечки по техническим каналам.

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	Семестр
		5
Контактная работа (по видам учебных занятий)	64	64
В том числе:		
– лекции (Л)	32	32
– практические занятия (ПЗ)	-	-
– лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС) (всего)	40	40
Контроль	4	4
Форма контроля (промежуточной аттестации)	3	3
Общая трудоемкость: час / з.е.	108/3	108/3

Примечание: «Форма контроля» – зачет (3)

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Классификация и краткая характеристика технических каналов утечки информации.	Лекция 1. Вводная лекция в область технической защиты информации (4 часа). Лекция 2. Угрозы безопасности информации. Лекция 3. Оптический канал утечки информации. Лекция 4. Акустический и виброакустический канал утечки информации. Лекция 5. Другие каналы утечки информации (4 часа).	ОПК-9.1.2 ОПК-9.2.2
		Лабораторная работа 1. Побочные электромагнитные излучения средств вычислительной техники. Лабораторная работа 2. Электромагнитные наводки от средств	ОПК-9.1.2 ОПК-9.2.2

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		<p>вычислительной техники в линейных коммуникациях.</p> <p>Лабораторная работа 3. Определение каналов утечки информации в помещении.</p> <p>Самостоятельная работа. Изучить учебное пособие Беляков И.А. Технические каналы утечки информации / И.А. Беляков – СПб: ФГБОУ ВО ПГУПС, 2017. – 33 с. Подготовиться к выполнению лабораторных работ.</p>	
2	Способы и средства защиты информации от утечки по техническим каналам.	<p>Лекция 6. Организация защиты информации на объектах информатизации.</p> <p>Лекция 7. Способы защиты информации от утечки по техническим каналам.</p> <p>Лекция 8. Средства защиты информации от утечки по техническим каналам.</p> <p>Лекция 9. Правовая база для организации защиты информации от утечки по техническим каналам.</p> <p>Лабораторная работа 4. Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу.</p> <p>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.</p>	<p>ОПК-9.1.2 ОПК-9.2.2</p> <p>ОПК-9.1.2 ОПК-9.2.2</p> <p>ОПК-9.1.2 ОПК-9.2.2</p>
3	Методы и средства контроля эффективности защиты информации от утечки по техническим каналам.	<p>Лекция 10. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.</p> <p>Лекция 11. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации.</p> <p>Лекция 12. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.</p> <p>Лекция 13. Методы и средства контроля эффективности защиты выделенных</p>	<p>ОПК-9.1.2 ОПК-9.2.2</p>

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		помещений от утечки речевой информации по техническим каналам. Лекция 14. Методы и средства выявления электронных устройств перехвата информации.	
		Лабораторная работа 5. Методы и средства контроля эффективности технической защиты информации.	ОПК-9.1.2 ОПК-9.2.2
		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. Подготовиться к выполнению лабораторных работ.	ОПК-9.1.2 ОПК-9.2.2

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Классификация и краткая характеристика технических каналов утечки информации	14	0	16	10	40
2	Способы и средства защиты информации от утечки по техническим каналам	8	0	8	20	36
3	Методы и средства контроля эффективности защиты информации от утечки по техническим каналам	10	0	8	10	28
	Итого	32	-	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.

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.

– 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» № 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
31 марта 2025 г.

М.Ф. Соломатова