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.28 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
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 «*Основы информационной безопасности» (Б1.О.28*) (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 основных понятий и нормативных документов в области защиты информации;
- изучение основных методов и подходов к защите информации в информационных системах;
- изучение основных психологических аспектов информационной безопасности и мер по защите.

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)**
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	
ОПК-1.1.1. Знает сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства; угрозы и источники угроз информационной безопасности, методы обеспечения информационной безопасности;	*Обучающийся знает:* основные понятия и нормативные документы в области защиты информации, основные угрозы безопасности информации в информационных системах, основные меры по защите информации в информационных системах

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
психологические аспекты информационной безопасности в современном обществе; профессиональную и криптографическую терминологию	
ОПК-1.2.1. Умеет применять основные методы обеспечения информационной безопасности	*Обучающийся умеет:* использовать основные методы управления защитой информации на базовом уровне
ОПК-1.3.1. Владеет базовой терминологией и гуманитарными аспектами в области информационной безопасности личности, общества и государства, а также базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности	*Обучающийся владеет* основными понятиями в области защиты информации, основными подходами к защите информации в информационных системах

3. Место дисциплины в структуре основной профессиональной образовательной программы

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

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		3
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), 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	Введение в информационную безопасность	Лекция 1.1 Введение в информационную безопасность	ОПК-1.1.1. ОПК-1.1.2. ОПК-1.3.1.
		Лекция 1.2. Понятие информации. Защищаемая информация	
		Лекция 1.3 Основные понятия информационной безопасности (4 час)	
		Лабораторная работа №1 «Изучение правовых аспектов деятельности в области информационной безопасности» (4 час)	
		Практическое задание №1 «Программное уничтожение и восстановление компьютерной информации» (4 час)	
		Лабораторная работа №2 «Изучение методов защиты информации» (4 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [1] – [3] Интернет-ресурсы [1] – [5]	
2	Введение в правила разграничения доступа	Лекция 2.1 Основные понятия ПРД	ОПК-1.1.3. ОПК-1.1.4. ОПК-1.2.1. ОПК-1.3.1. ОПК-1.3.2.
		Лекция 2.2 Идентификация	
		Лекция 2.3 Аутентификация	
		Лекция 2.4 Введение в модели разграничения доступа	
		Лабораторные работы №3, 4 «Обеспечение информационной безопасности предприятия. Применение методов защиты информации» (12 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [3] Дополнительная литература: [1], [2] Нормативные документы: [1] – [6] Интернет-ресурсы [1] – [5]	
3	Введение в криптографические методы защиты	Лекция 3.1 Стеганографические методы защиты.	ОПК-1.1.3. ОПК-1.1.4. ОПК-1.2.1.
		Лекция 3.2 Методы подстановки и	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
	информации	перестановки.	ОПК-1.3.1. ОПК-1.3.2.
		Лекция 3.3 Гаммирование.	
		Лекция 3.4 Хеширование	
		Практическое задание №2 «Основы стеганографии» (6 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [3] Дополнительная литература: [1], [2] Нормативные документы: [1] – [6] Интернет-ресурсы [1] – [5]	
4	Принципы построения системы защиты информации	Лекция 4.1 Составляющие системы защиты информации.	ОПК-1.1.3. ОПК-1.1.4. ОПК-1.2.1. ОПК-1.3.1. ОПК-1.3.2.
		Лекция 4.2 Подходы к построению системы защиты информации от угроз конфиденциальности.	
		Лекция 4.3 Подходы к построению системы защиты информации от угроз целостности.	
		Лекция 4.4 Подходы к построению системы защиты информации от угроз доступности.	
		Лабораторная работа №5 «Простое шифрование» (18 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [3] Дополнительная литература: [1], [2] Нормативные документы: [1] – [6] Интернет-ресурсы [1] – [5]	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Введение в информационную безопасность	8	12		6	26
2	Введение в правила разграничения доступа	8	12		6	26
3	Введение в криптографические методы защиты информации.	8	6		6	20
4	Принципы построения системы защиты информации	8	18		10	36
	Итого	32	48		28	108

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
					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, 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. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с.

2. Диасамидзе С.В., Бубнов В.П. Гуманитарные основы информационной безопасности: учебное пособие. – СПб: ПГУПС, 2018. – 48 с.

3. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] : учеб.пособие — Электрон. дан. — Москва : , 2016. — 266 с. — Режим доступа: https://e.lanbook.com/book/100295

4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2010. - 544 с.https://e.lanbook.com/book/1122

5. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

6. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы

7. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ;

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, *доцент* _____ *С.В. Корниенко*
23.01.2026 г.