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.29 «ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
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 *«Гуманитарные аспекты информационной безопасности» (Б1.О.29*) (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 и информационно-психологической безопасности;
- изучение информационно-психологических аспектов безопасности, основных угроз информационной безопасности современного общества и основных мер по противодействию информационно-психологическим угрозам.

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; психологические аспекты	*Обучающийся знает:* сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства; психологические аспекты информационной безопасности в современном обществе;

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
информационной безопасности в современном обществе; профессиональную и криптографическую терминологию	
ОПК-1.2.1. Умеет применять основные методы обеспечения информационной безопасности	*Обучающийся умеет:* применять основные меры по противодействию информационно-психологическим угрозам
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 и гуманитарными аспектами в области информационной безопасности личности, общества и государства, основными мерами по противодействию информационно-психологическим угрозам

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
		4
Контактная работа (по видам учебных занятий) В том числе:	64	64
– 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)	З	З
Общая трудоемкость: час / з.е.	108 / 3	108 / 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	Информационно-психологическое воздействие в современном мире	Лекция 1.1 Воздействие средств массовой информации (4 час)	ОПК-1.1.1. ОПК-1.1.2. ОПК-1.1.4. ОПК-1.2.1. ОПК-1.3.1. ОПК-1.3.2.
		Лекция 1.2 Социальный инжиниринг (4 час)	
		Лекция 1.3 Социальные сети (4 час)	
		Лекция 1.4 Информационно-психологическое воздействие и методы защиты (4 час)	
		Лабораторная работа №1 «Фейковые новости» (4 час)	
		Лабораторная работа №2 «Противодействие методам социального инжиниринга» (6 час)	
		Лабораторная работа №3 «Противодействие манипулированию» (6 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче зачета). Литература: [1] – [8] Интернет-ресурсы [1] – [5]	
2	Информационная война	Лекция 2.1 Информационное противостояние в современном мире (4 час)	ОПК-1.1.1. ОПК-1.1.2. ОПК-1.1.4. ОПК-1.2.1. ОПК-1.3.1. ОПК-1.3.2.
		Лекция 2.2 Государственная политика РФ в информационной сфере (4 час)	
		Лекция 2.3 Кибервойна (4 час)	
		Лекция 2.4 Информационное оружие (4 час)	
		Лабораторная работа № 4 «Информационная война» (6 час)	
		Лабораторная работа № 5 «Форензика» (10 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче зачета). Литература: [1] – [8] Интернет-ресурсы [1] – [5]	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Информационно-	16		16	20	60

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
	психологическое воздействие в современном мире					
2	Информационная война	16		16	20	44
	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" - 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. Вирен, Г. Современные медиа: Приемы информационных войн: Учеб.пособие для студентов вузов. [Электронный ресурс] — Электрон.дан. — М. : Аспект Пресс, 2013. — 126 с. — Режим доступа: http://e.lanbook.com/book/68804

4. Малюк, А.А. Этика в сфере информационных технологий. [Электронный ресурс] / А.А. Малюк, О.Ю. Полянская, И.Ю. Алексеева. — Электрон.дан. — М. : Горячая линия-Телеком, 2011. — 288 с. — Режим доступа: http://e.lanbook.com/book/5172

5. Манойло, А.В. Государственная информационная политика в условиях информационно-психологической войны. [Электронный ресурс] / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. — Электрон.дан. — М. : Горячая линия-Телеком, 2012. — 340 с. — Режим доступа: http://e.lanbook.com/book/5175

6. Новиков, В.К. Информационное оружие – оружие современных и будущих войн. [Электронный ресурс] — Электрон.дан. — М. : Горячая линия-Телеком, 2013. — 262 с. — Режим доступа: http://e.lanbook.com/book/11840

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

8. 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*
31.03.2025 г.