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.19 «*ЗАЩИТА ИНФОРМАЦИИ*»
для направления подготовки
09.03.01 «*Информатика и вычислительная техника*»

по профилю
«*Программное обеспечение средств вычислительной техники и автоматизированных систем*»

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» К.З. Билятдинов
28 января 2026 г.

СОГЛАСОВАНО

Руководитель ОПОП С.Г. Ермаков
28 января 2026 г.

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*Защита информации» (Б1.О.19*) (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности *09.03.01 «Информатика и вычислительная техника*» (далее – ФГОС ВО), утвержденного 19 сентября 2017 г., приказ Минобрнауки России № 929.

Целью изучения дисциплины является формирование у обучающихся способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; разрабатывать алгоритмы и программы, пригодные для практического применения.

Для достижения цели дисциплины решаются следующие задачи:

- изучение обучающимися гуманитарных аспектов информационной безопасности, методов и средств криптографической защиты информации, программно-аппаратных методов и средств защиты информации;
- обретение обучающимися умений и навыков выявления уязвимостей информационных систем, определения наиболее значимых угроз информационной безопасности, использования статистических характеристик открытых и зашифрованных сообщений для оценивания криптостойкости симметричных шифров, применения криптографических возможностей языка программирования высокого уровня для защиты данных в прикладных программах.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Планируемыми результатами обучения по дисциплине (модулю) 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**
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-3.1. Знает принципы, методы и средства решения стандартных задач	Обучающийся *знает*: – основные категории информационной безопасности; – основы правовой защиты информации; – основы организационного обеспечения информационной безопасности; – основы информационно-психологической безопасности; – модель и математические характеристики симметричных шифров; – алгоритмы шифрования и имитозащиты сообщений в симметричных криптосистемах; – протоколы шифрования с открытым ключом и защищенной передачи ключей; – схемы формирования и проверки электронной подписи; – методы и средства идентификации, аутентификации,

Индикаторы достижения компетенций	Результаты обучения по дисциплине
	разграничения доступа; – методы и средства обеспечения информационной безопасности при работе в компьютерных сетях.
ОПК-3.2. Умеет предлагать новые идеи и подходы к решению инженерных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Обучающийся *умеет*: – выявлять уязвимости информационной системы и определять возможные угрозы информационной безопасности; – анализировать содержание нормативно-правовых документов в области информационной безопасности; – использовать статистические характеристики открытых и зашифрованных сообщений для оценивания криптостойкости симметричных шифров; – применять криптографические возможности языков программирования высокого уровня для защиты данных в прикладных программах.
ОПК-3.3. Имеет навыки подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями	Обучающийся *имеет навыки*: – подготовки отчетов о выполнении работ.

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)	64 32 - 32
Самостоятельная работа (СРС) (всего)	44
Контроль	36
Форма контроля (промежуточной аттестации)	Э
Общая трудоемкость: час / з.е.	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	Гуманитарные аспекты информационной безопасности	Лекция 1.1 Информационная безопасность и защиты информации: основные категории Лекция 1.2 Основы правовой защиты информации Лекция 1.3 Основы организационного обеспечения информационной безопасности Лекция 1.4 Информационно-психологическая безопасность Лабораторная работа № 1.1 (4 часа) Угрозы информационной безопасности и уязвимости информационной системы Лабораторная работа № 2.1 (4 часа) Изучение правовых аспектов деятельности в области информационной безопасности Самостоятельная работа Повторение лекционного материала, подготовка к выполнению лабораторных работ, подготовка к прохождению теста по дисциплине	ОПК-3.1, ОПК-3.2, ОПК-3.3
2	Методы и средства криптографической защиты информации	Лекция 2.1 Модель и математические характеристики симметричных шифров Лекция 2.2 Поточные шифры Лекция 2.3 Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Магма» Лекция 2.4 Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Кузнечик»	ОПК-3.1, ОПК-3.2, ОПК-3.3

		Лекция 2.5 Режимы использования блочных шифров Лекция 2.6 Асимметричные криптосистемы. Протоколы шифрования с открытым ключом и защищенной передачи ключей Лекция 2.7 Схемы ЭП на основе вычислений по RSA-модулю и в конечном поле Лекция 2.8 Схема ЭП на основе вычислений в группе точек эллиптической кривой Лекция 2.9 Инфраструктура открытых ключей Лабораторная работа № 2 (4 часа) Использование статистических характеристик открытых и зашифрованных сообщений для оценивания криптостойкости симметричных шифров Лабораторная работа № 2.1 (2 часа) Изучение простейших методов шифрования информации в ручном режиме Лабораторная работа № 2.2 (8 часов) Использование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Симметричное шифрование. Исследование статистических свойств открытого и зашифрованного текста Лабораторная работа № 2.3 (8 часов) Использование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Защищенный обмен ключами Лабораторная работа № 2.4 (6 часов)	

		Использование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Электронная подпись <u>Самостоятельная работа</u> Повторение лекционного материала, подготовка к выполнению лабораторных работ, подготовка к прохождению теста по дисциплине	
3	Программно-аппаратные методы и средства защиты информации	<u>Лекция 3.1</u> Программно-аппаратные средства идентификации, аутентификации, управления доступом <u>Лекция 3.2</u> Программно-аппаратные средства защиты информации в компьютерных сетях <u>Самостоятельная работа</u> Повторение лекционного материала, подготовка к прохождению теста по дисциплине	ОПК-3.1, ОПК-3.2, ОПК-3.3

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Гуманитарные аспекты информационной безопасности	8	0	8	6	22
2	Методы и средства криптографической защиты информации	14	0	24	34	72
3	Программно-аппаратные методы и средства защиты информации	10	0	0	4	14
	Итого	32	0	32	44	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 являются 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, предусмотренных 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 бакалавриата, 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 криптографической защиты информации, 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:

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://urait.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.

– 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: учебник: / С.Е. Ададуров и др.; под ред. А.А. Корниенко. – Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте – М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. – 440 с.
2. Информационная безопасность и защита информации на железнодорожном транспорте: учебник: / А.А. Корниенко и др.; под ред. А.А. Корниенко. – Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте –М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. – 448 с.
3. Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс]: Учебные пособия — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578.
4. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] : Учебные пособия — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с. — Режим доступа: http://e.lanbook.com/book/3032.
5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 33 с.
6. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.
7. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.
8. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

8.6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых в образовательном процессе:

– Личный кабинет ЭИОС [Электронный ресурс]. – URL: my.pgups.ru — Режим доступа: для авториз. пользователей;

– Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://sdo.pgups.ru — Режим доступа: для авториз. пользователей;

– Научно-техническая библиотека университета [Электронный ресурс]. – Режим доступа: http://library.pgups.ru/ (свободный доступ);

– Гарант Информационно-правовой портал [Электронный ресурс] – Режим доступа: http://www.garant.ru.

Разработчик рабочей программы, *доцент* *М.Л. Глухарев*
19.01.2026 г.