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.32 «*МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ*»

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 «*Методы и средства криптографической защиты информации» (Б1.О.32*) (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 использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Для достижения цели дисциплины решаются следующие задачи:

- формирование о обучающихся знаний о криптографических методах, алгоритмах, протоколах, используемых для защиты информации в автоматизированных системах;
- формирование у обучающихся умений, связанных с разработкой и анализом программных моделей средств криптографической защиты информации;
- формирование у обучающихся навыков использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

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.

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

- использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	
ОПК-10.1.1. Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	Обучающийся *знает*: – общие сведения о криптографических методах и алгоритмах защиты информации в автоматизированных системах; – модель и математические характеристики симметричных шифров, криптографические примитивы; – алгебраические и вероятностные свойства подстановочных преобразований;

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
	– современные блочные, поточные и композиционные шифры; – основы асимметричных криптосистем; – системы шифрования с открытым ключом и получения общего секретного ключа; – схемы формирования и проверки электронной подписи; – особенности применения хеш-функций в криптографии; – методы аутентификации открытых ключей, способы построения инфраструктуры открытых ключей; – протоколы формирования и проверки коллективной, композиционной и «слепой» электронной подписи; – протоколы аутентификации участников информационного обмена; – протоколы управления ключами; – пороговые схемы разделения и восстановления секретов; – перспективы развития криптографических протоколов.
ОПК-10.2.1. Умеет разрабатывать и анализировать программные модели средств криптографической защиты информации	Обучающийся *умеет*: – разрабатывать и анализировать программные модели средств криптографической защиты информации, основанных на симметричных алгоритмах шифрования; – исследовать алгебраические и вероятностные свойства криптографических примитивов; – разрабатывать программные модели блочных симметричных шифров, используемых в различных режимах; – разрабатывать и анализировать программные модели средств шифрования с открытым ключом, бесключевого шифрования и открытого распределения ключей; – разрабатывать и анализировать программные модели средств электронной подписи.
ОПК-10.3.1. Имеет навыки использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач	Обучающийся *имеет навыки*: – использования и исследования криптографических сервис-провайдеров при решении задач профессиональной деятельности; – использования криптографических утилит при решении задач профессиональной деятельности.

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	Модуль	
		1	2
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	 64 - 80	 32 - 48	 32 - 32
Самостоятельная работа (СРС) (всего)	68	28	40
Контроль	40	36	4
Форма контроля (промежуточной аттестации)		Э	З
Общая трудоемкость: час / з.е.	252/7	144/4	108/3

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
Модуль 1 (5 семестр)			
1	Общие сведения о криптографии	Лекция 1.1. Общие сведения о криптографических методах и алгоритмах защиты информации в автоматизированных системах	ОПК-10.1.1, ОПК-10.2.1
		Лабораторная работа № 1.1 (ознакомительная). Изучение простейших криптографических преобразований (4 часа)	
		Самостоятельная работа: – изучение раздела 1 части 1 учебного пособия [1]; – подготовка к тесту по лекционному материалу 5 семестра[1].	ОПК-10.1.1, ОПК-10.2.1
2	Симметричные криптосистемы	Лекция 2.1. Модель и математические характеристики симметричных шифров. Криптографические примитивы	ОПК-10.1.1, ОПК-10.2.1
		Лекция 2.2. Алгебраические и вероятностные свойства подстановочных преобразований	
		Лекция 2.3. Современные блочные, поточные и композиционные шифры (10 часов)	
		Лабораторная работа № 2.1 (ознакомительная). Изучение статистических характеристик симметричных шифров	ОПК-10.1.1, ОПК-10.2.1

[1] Подготовка к тесту включает прохождение обучающего теста, размещенного на странице курса в электронной информационно-образовательной среде (сайт sdo.pgups.ru).

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лабораторная работа № 2.2 (отчетная). Разработка и анализ программных моделей средств криптографической защиты информации, основанных на симметричных алгоритмах шифрования (4 часа)	
		Лабораторная работа № 2.3 (ознакомительная). Алгебраические и вероятностные свойства криптографических примитивов (2 часа)	
		Лабораторная работа № 2.4 (отчетная) Исследование алгебраических и вероятностных свойств подстановочного преобразования (6 часов)	
		Лабораторная работа № 2.5 (отчетная). Разработка программной модели блочного симметричного шифра, используемых в различных режимах (8 часов)	
		Самостоятельная работа: – изучение раздела 2 части 1 учебного пособия [1]; – изучение стандартов [4], [5]; – подготовка к выполнению лабораторных работ; – подготовка к тесту по лекционному материалу 5 семестра.	ОПК-10.1.1, ОПК-10.2.1
3	Асимметричные криптосистемы	Лекция 3.1. Основы асимметричных криптосистем	ОПК-10.1.1, ОПК-10.2.1
		Лекция 3.2. Системы шифрования с открытым ключом и получения общего секретного ключа	
		Лекция 3.3. Схемы формирования и проверки электронной подписи (8 часов)	
		Лекция 3.4. Особенности применения хеш-функций в криптографии	
		Лекция 3.5. Методы аутентификации открытых ключей, способы построения инфраструктуры открытых ключей	
		Лабораторная работа № 3.1 (отчетная). Разработка и анализ программных моделей средств шифрования с открытым ключом, бесключевого шифрования и открытого распределения ключей (10 часов)	ОПК-10.1.1, ОПК-10.2.1
		Лабораторная работа № 3.2 (отчетная). Разработка и анализ программных моделей средств электронной подписи (12 часов)	
		Самостоятельная работа: – изучение части 2 учебного пособия [1]; – изучение стандартов [6], [7]; – подготовка к выполнению лабораторных работ; – подготовка к тесту по лекционному материалу 5 семестра.	ОПК-10.1.1, ОПК-10.2.1

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
Модуль 2 (6 семестр)			
4	Средства криптографической защиты информации	Лекция 4.1. Криптографические провайдеры	ОПК-10.1.1, ОПК-10.3.1
		Лекция 4.2. Криптографические механизмы Java (4 часа)	
		Лекция 4.3. Криптографические утилиты	
		Лабораторная работа № 5.1. Использование и исследование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Симметричное шифрование (8 часов)	
		Лабораторная работа № 5.2. Использование и исследование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Защищенный обмен ключами (12 часов)	
		Лабораторная работа № 5.3. Использование и исследование криптографических сервис-провайдеров при решении задач профессиональной деятельности. Электронная подпись (12 часов)	
		Самостоятельная работа: – подготовка к выполнению лабораторных работ.	
5	Криптографические протоколы	Лекция 5.1. Схемы коллективной и композиционной электронной подписи (2 часа)	ОПК-10.1.1, ОПК-10.2.1
		Лекция 5.2. Слепая электронная подпись (2 часа)	
		Лекция 5.3. Криптографические протоколы аутентификации (2 часа)	
		Лекция 5.4. Протоколы доказательства с нулевым разглашением (2 часа)	
		Лекция 5.5. Протоколы управления криптографическими ключами. Протоколы TLS, Kerberos (4 часа)	
		Лекция 5.6. Схемы разделения и восстановления секретов (2 часа)	
		Лекция 5.7. Протоколы электронной жеребьёвки (2 часа)	
		Лекция 5.8. Блокчейн (2 часа)	
		Лекция 5.9. Гомоморфное шифрование (2 часа)	
		Лекция 4.5. Перспективы развития криптографических протоколов (4 часа)	
		Самостоятельная работа: – изучение материала учебного пособия [2]; – подготовка к тесту по лекционному материалу 6 семестра.	ОПК-10.1.1, ОПК-10.2.1

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
Модуль 1 (5 семестр)						
1	Общие сведения о криптографии	2	0	4	2	4
2	Симметричные криптосистемы	14	0	22	12	50
3	Асимметричные криптосистемы	16	0	22	14	54
	Итого	32	0	32	28	108
					Контроль	36
					Всего (общая трудоемкость, час.)	144

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
Модуль 2 (6 семестр)						
4	Средства криптографической защиты информации	8	0	32	20	52
5	Криптографические протоколы	24	0	0	20	52
	Итого	32	0	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.

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:

– MS Office;
– Операционная система Windows;
– Антивирус Касперский;
– Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/);
– Oracle Java SE Development Kit 8, в том числе встроенные в JRE криптографические сервис-провайдеры (бесплатное, свободно распространяемое программное обеспечение; режим доступа http://www.oracle.com/technetwork/java/javase/downloads/index.html)
– NetBeans IDE 8.2 (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://netbeans.org/downloads/);
– бесплатные, свободно распространяемые среды программ на языке Python (пакет Anaconda, режим доступа https://www.anaconda.com; Python IDLE, режим доступа https://www.python.org/);
– криптографическая библиотека OpenSSL (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://www.openssl.org/).

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.

– Техническая документация по языку программирования Python [Электронный ресурс] – Режим доступа: https://www.python.org/doc/ (свободный доступ).

– 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. А. А. Корниенко, М. Л. Глухарев. Криптографические методы защиты информации: учебное пособие.

Ч. 1. – СПб.: ФГБОУ ВО ПГУПС, 2017. – 64 с.

Ч. 2. – СПб.: ФГБОУ ВО ПГУПС, 2018. – 63 с.

2. А. А. Корниенко, М. Л. Глухарев. Криптографические протоколы: учебное пособие. – СПб.: ФГБОУ ВО ПГУПС, 2020. – 74 с.

3. Г. И. Кожомбердиева, М. Л. Глухарев. Криптографическая защита информации и управление доступом на платформе Java: учебное пособие. – СПб.: ФГБОУ ВПО ПГУПС, 2016. - 86 с.

4. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.

5. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

6. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 33 с.

7. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.

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;

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

Разработчик рабочей программы, *доцент* *М.Л. Глухарев*
16.03.2025 г.