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

«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ» (Б1.Б.12)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Информационная безопасность автоматизированных систем на транспорте»

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и обсуждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 10 от «24» апреля 2018 г.

Заведующий кафедрой «Информатика и информационная безопасность»
«24» апреля 2018 г. _____ А. А. Корниенко

СОГЛАСОВАНО

Руководитель ОПОП
«24» апреля 2018 г. _____ А. А. Корниенко

Председатель методической комиссии факультета «Автоматизация и интеллектуальные технологии»
«24» апреля 2018 г. _____ М. Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «01» декабря 2016 г., приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем», по дисциплине «Криптографические методы защиты информации».

Целью изучения дисциплины является формирование у обучающегося общепрофессиональных и профессиональных компетенций (см. раздел 2), позволяющих корректно применять аппарат алгебры (конкретно – теории чисел) в профессиональной деятельности, проводить контрольные проверки криптографических средств защиты информации, разрабатывать научно-техническую документацию, отчеты, обзоры, публикации в рассматриваемой области.

Для достижения поставленной цели решаются следующие задачи:

– формирование у обучающихся знаний, умений и навыков, приводимых в разделе 2 настоящей рабочей программы;

– подготовка обучающихся к освоению других дисциплин, формирующих те же компетенции;

– подготовка обучающихся к прохождению преддипломной практики и государственной итоговой аттестации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- типовые поточные и блочные шифры;
- частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
- типовые шифры с открытыми ключами;
- модели шифров и математические методы их исследования;
- основные свойства схем шифрования, электронной подписи, аутентификации, разделения секретов при решении задач защиты технологического электронного документооборота и документоведения.

УМЕТЬ:

- эффективно использовать криптографические методы и средства

защиты информации в автоматизированных системах;
- применять математические методы исследования моделей шифров;
- обеспечивать защиту электронного технологического документооборота на основе электронной подписи;
- решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей;
- проводить анализ качества (стойкости) криптографических преобразований.

ВЛАДЕТЬ:
- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии.

Приобретенные знания, умения, навыки и/или опыт деятельности, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 основной профессиональной образовательной программы (ОПОП).

Изучение дисциплины направлено на формирование следующих **общепрофессиональных компетенций (ОПК)**:

– *способности корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники* (ОПК-2).

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

научно-исследовательская деятельность:

– *способности разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ* (ПК-7);

контрольно-аналитическая деятельность:

– *способности проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации* (ПК-14).

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 общей характеристики ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 общей характеристики ОПОП.

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Криптографические методы защиты информации» (Б1.Б.12) относится к базовой части и является обязательной для изучения.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр	
		7	8
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	114 48 - 66	64 32 - 32	50 16 - 34
Самостоятельная работа (СРС) (всего)	93	35	58
Контроль	45	9	36
Форма контроля знаний		зачет	экзамен, курсовая работа
Общая трудоемкость: час / з.е.	252/7	108/3	144/4

5. Содержание и структура дисциплины

5.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Общие сведения о криптографии	1.1. Предмет, задачи и содержание дисциплины. 1.2. Основные термины и определения криптографии. Виды криптографической защиты информации. 1.3. История криптографии. 1.4. Классификация криптосистем. 1.5. Понятие криптостойкости. Общие сведения о криптоанализе.
2	Симметричные криптосистемы	2.1. Модель и математические характеристики симметричных шифров Модель симметричного шифра по К. Шеннону. Безусловно и условно стойкие симметричные шифры.

		2.2. Подстановочные и перестановочные преобразования в симметричных шифрах Моноалфавитная подстановка. Полиалфавитная подстановка. Омофоническая и полиграммная подстановки. Простая перестановка. Маршрутная перестановка. Табличная перестановка. 2.3. Алгебраические и корреляционные свойства подстановочных преобразований Представление подстановочного преобразования блока данных в виде векторной булевой функции (БФ). Преобразование Уолша-Адамара. Сбалансированность БФ. Корреляционные свойства БФ. Критерии распространения изменений для БФ. Исследование нелинейности БФ. Методика оценки качества подстановочных преобразований. 2.4. Методы криптоанализа простейших шифров Статистическая криптоатака. Криптоатака методом вероятного слова. Метод криптоатаки «встречи посередине». Методы криптоанализа перестановочных шифров. Требования к современным композиционным симметричным шифрам. 2.5. Поточные шифры Основы поточного шифрования. Синхронные и самосинхронизирующиеся поточные шифры. Генераторы псевдослучайных числовых последовательностей на основе регистров сдвига с линейной обратной связью. 2.6. Современные композиционные симметричные шифры Сеть Фейстеля. Криптосистема DES и ее модификации. Общие сведения о дифференциальном и линейном криптоанализе.

		2.7. Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015 Шифр «Магма». Виды преобразования информации в шифре «Кузнечик». Базовые алгоритмы зашифрования и расшифрования, процедура получения раундовых подключей в шифре «Кузнечик». 2.8. Режимы использования современных композиционных шифров. Стандарт ГОСТ Р 34.13-2015 Использование блочных шифров в режиме простой замены. Использование блочных шифров в режиме гаммирования. Использование блочных шифров в режиме гаммирования с обратной связью по выходу. Использование блочных шифров в режиме гаммирования с обратной связью по шифртексту. Использование блочных шифров в режиме простой замены с зацеплением. Использование блочных шифров в режиме выработки имитовставки. 2.9. Международный стандарт симметричного шифрования AES Общая характеристика AES. Описание алгоритма шифрования согласно AES. Процедура получения раундовых подключей в AES. Криптостойкость AES.
3	Асимметричные криптосистемы	3.1. Основы асимметричных криптосистем Принципы построения и функционирования асимметричных криптосистем. Классификация асимметричных криптосистем. Математические основы асимметричных криптосистем: термины и определения, утверждения и теоремы теории групп. 3.2. Системы шифрования с открытым ключом и получения общего секретного ключа Криптосистема RSA. Протокол получения общего секретного ключа Диффи-Хеллмана. Протокол открытого шифрования Эль-Гамаля. Протокол «бесключевого шифрования» Месси-Омуры.

		3.3. Общие сведения об электронной подписи Понятие электронной подписи (ЭП). Основные положения Федерального закона «Об электронной подписи». особенности усиленной ЭП. Терминологические вопросы: ЭП и электронная цифровая подпись. Требования к хеш-функциям в схемах ЭП. Виды атак на схемы ЭП. 3.4. Схемы ЭП на основе вычислений по RSA-модулю Схема ЭП Ривеста-Шамира-Адлемана (RSA). Схема ЭП М. Рабина. Схема ЭП Фиата-Шамира. 3.5. Схемы ЭП на основе вычислений в конечном поле Схемы ЭП на основе вычислений в конечном поле без сокращения размера подписи. Схема ЭП Т. Эль-Гамаля. Математические основы схем ЭП с сокращением размера подписи. Схема ЭП DSA. Схема ЭП К. Шнорра. 3.6. Схемы ЭП на основе вычислений в группе точек эллиптической кривой Математические основы эллиптической криптографии. Схемы формирования и проверки ЭП на основе ГОСТ Р 34.10-2012. 3.7. Хеш-функции в криптографии Типовые схемы хеш-функций. Стандарт хеширования ГОСТ Р 34.11-2012. Схемы хеширования серии MDx. Схемы хеширования SHA. 3.8. Инфраструктура открытых ключей Сертификат ключа. Понятие инфраструктуры открытых ключей. Компоненты инфраструктуры открытых ключей и их функции. Верификация цепочки сертификатов.

		Стандарты в области инфраструктуры открытых ключей.
4	Криптографические протоколы	4.1. Схемы коллективной и композиционной ЭП Понятие коллективной ЭП. Схема коллективной ЭП RSA. Схема коллективной ЭП на основе вычислений в конечном поле. Схема коллективной ЭП на основе вычислений в группе точек эллиптической кривой. Понятие композиционной ЭП. Схема композиционной ЭП RSA. Схема композиционной ЭП на основе вычислений в конечном поле. Схема композиционной ЭП на основе вычислений в группе точек эллиптической кривой. 4.2. Схемы слепой ЭП Понятие слепой подписи. Схема Д. Чаума. Слепая подпись на основе схемы ЭП Шнорра. 4.3. Протоколы аутентификации Понятие аутентификации и идентификации. Схемы аутентификации на основе симметричных алгоритмов шифрования. 4.4. Протоколы аутентификации с нулевым разглашением Протокол Фейге-Фиата-Шамира. Протокол Гиллоу-Куискуотера. 4.5. Протоколы управления ключами Метод генерации криптографических ключей по стандарту ANSI X9.17. Безопасное хранение, учет и удаление криптографических ключей. Иерархия ключей. Протокол распределения симметричных ключей без участия центра распределения ключей. Протокол распределения асимметричных ключей с участием центра распределения ключей. 4.6. Пороговые схемы разделения секретов Понятие (n, k)-пороговой схемы разделения секрета. Схема Шамира. Схема Асмута-Блума. 4.7. Перспективы развития криптографических

		4.7. Перспективы развития криптографических протоколов Протокол электронной жеребьевки. Протоколы «честной раздачи карт». «Временной замок» Ривеста-Шамира-Вагнера. Квантовая криптография. Постквантовая криптография. Гомоморфное шифрование. «Легковесная» криптография.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Общие сведения о криптографии	2	-	-	1
2	Симметричные криптосистемы	18	-	20	20
3	Асимметричные криптосистемы	12	-	12	14
4	Криптографические протоколы	16	-	34	58
Итого		48	-	66	93

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1	Общие сведения о криптографии	Основная литература: [1], [3]
2	Симметричные криптосистемы	Основная литература: [1], [3] Дополнительная литература: [1] Нормативные документы: [2], [3] Другие издания: [3], [4]
3	Асимметричные криптосистемы	Основная литература: [1], [2] Дополнительная литература: [1] Нормативные документы: [1] Другие издания: [1], [2], [4]
4	Криптографические протоколы	Основная литература: [1] Дополнительная литература: [1] Другие издания: [1], [2], [4]

7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств по дисциплине является неотъемлемой частью рабочей программы и представлен отдельным документом,

рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

8. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для освоения дисциплины

8.1 Перечень основной учебной литературы, необходимой для освоения дисциплины

1. Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте [Электронный ресурс] : учеб. — Электрон. дан. — Москва : УМЦ ЖДТ, 2014. — 440 с. — Режим доступа: https://e.lanbook.com/book/59240.
2. Шаньгин В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон. дан. — М.: ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578.
3. Криптографические методы защиты информации. Ч. 1: учеб. пособие / А. А. Корниенко, М. Л. Глухарев. – СПб.: ФГБОУ ВО ПГУПС, 2017. – 64 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Средства защиты информации на железнодорожном транспорте (криптографические методы и средства) [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : УМЦ ЖДТ, 2006. — 256 с. — Режим доступа: https://e.lanbook.com/book/59239.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.
2. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.
3. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

8.4 Другие издания, необходимые для освоения дисциплины

1. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб.: БХВ-Петербург, 2007. – 304 с.
2. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. – СПб.: БХВ-Петербург, 2010. – 304 с.

3. К. Шеннон. Теория связи в секретных системах – пер. с англ. В. Ф. Писаренко. - [Электронный ресурс] – Режим доступа: http://pv.bstu.ru/crypto/shannon.pdf

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002. – 816 с.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Личный кабинет обучающегося и электронная информационно-образовательная среда [Электронный ресурс]. – Режим доступа: http://sdo.pgups.ru/ (для доступа к полнотекстовым документам требуется авторизация).

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

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

10. 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 с помощью учебно-методического обеспечения, приведенного в разделах 6, 8 и 9 рабочей программы.

2. Для формирования компетенций обучающийся должен представить выполненные типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем (см. фонд оценочных средств по дисциплине).

3. По итогам текущего контроля по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. фонд оценочных средств по дисциплине).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

- персональные компьютеры, локальная вычислительная сеть кафедры, проектор;

- методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийных материалов;
- лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;
- Интернет-сервисы и электронные ресурсы: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося – поисковые системы, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

- операционная система Windows, MS Office, 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 (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/).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Материально-техническая база обеспечивает проведение всех видов учебных занятий, предусмотренных учебным планом по данной специальности, и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

- помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в

соответствии с рабочей программой дисциплины;

– лабораторию программно-аппаратных средств обеспечения информационной безопасности (ауд. 2-105), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО, в том числе криптографическими средствами защиты информации; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;

– помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;

– помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации;

– помещения для проведения групповых и индивидуальных консультаций, укомплектованные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых программных средств (см. раздел 11);

– помещения для проведения текущего контроля и промежуточной аттестации.

Разработчик программы, доцент _____ М. Л. Глухарев

«20» апреля 2018 г.