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
«ЗАЩИТА ИНФОРМАЦИИ» (Б1.Б.13)
для направления
09.03.01 «Информатика и вычислительная техника»
по профилю
«Программное обеспечение средств вычислительной техники и
автоматизированных систем»
(академический бакалавриат, прикладной бакалавриат)

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена, 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

Заведующий кафедрой «Информационные и вычислительные системы»
«25» апреля 2018 г. _____ А. Д. Хомоненко

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

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «12» января 2016 г., приказ № 5 по направлению 09.03.01 «Информатика и вычислительная техника», по дисциплине «Защита информации».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других дисциплин в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника общекультурных, общепрофессиональных и профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности (научно-исследовательская, научно-педагогическая, проектно-конструкторская, проектно-технологическая) и профилем «Программное обеспечение средств вычислительной техники и автоматизированных систем».

Для достижения поставленной цели решаются следующие задачи:

- подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
- развитие социально-воспитательного компонента учебного процесса.

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

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

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

- сущность и понятие информации, информационной безопасности и кибербезопасности, свойства защищенности информации;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
- цели и задачи в области обеспечения информационной безопасности на железнодорожном транспорте;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- 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;
- программно-аппаратные средства обеспечения информационной безопасности в автоматизированных информационных системах, системах управления базами данных, компьютерных сетях.

УМЕТЬ:

- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
- применять средства обеспечения безопасности данных.

ВЛАДЕТЬ:

- навыками своевременного и точного выявления актуальных угроз информационной безопасности объекта информатизации;
- навыками использования интерфейсов прикладных программ для реализации прикладных функций криптографической защиты информации и управления доступом в создаваемых программных продуктах;
- навыками своевременного предотвращения и выявления уязвимостей разрабатываемого программного обеспечения;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

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 **общекультурных компетенций (ОК)**:

- *способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия* (ОК-5).

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

- *способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* (ОПК-5).

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

научно-педагогическая деятельность:

- *способность готовить конспекты и проводить занятия по обучению работников применению программно-методических комплексов, используемых на предприятиях* (ПК-4).

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 «Защита информации» (Б1.Б.13) относится к базовой части и является обязательной дисциплиной.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		7
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – лабораторные работы (ЛР)	64 32 32	64 32 32
Самостоятельная работа (СРС) (всего)	71	71
Контроль	45	45
Форма контроля знаний	Э	Э
Общая трудоемкость: час / з.е.	180/5	180/5

5. Содержание и структура дисциплины

5.1 Содержание дисциплины

№ П/П	Наименование раздела дисциплины	Содержание раздела
1	Введение в дисциплину	Основные понятия и определения дисциплины. Цели и задачи обеспечения ИБ на железнодорожном транспорте. Кибербезопасность.
2	Угрозы информационной безопасности и уязвимости автоматизированных информационных систем	Угрозы информационной безопасности. Классификация угроз и их источников. Неформальная модель нарушителя. Уязвимости автоматизированных информационных систем.
3	Общая характеристика и классификация методов защиты информации	Цели и методы защиты информации. Правовые методы обеспечения ИБ. Обзор методов защиты информации от утечки по техническим каналам связи. Обзор организационно-технических и экономических методов защиты информации.
4	Введение в криптографию	Виды криптографического преобразования информации. Классификация криптосистем. Понятия криптостойкости, криптоанализа и криптоатаки. Классификация криптосистем по криптостойкости.
5	Модель и математические характеристики симметричных шифров	Модель симметричного шифра. Статистические характеристики источников сообщений. Расстояние единственности как характеристика криптостойкости шифра. Абсолютно стойкий шифр по Шеннону.
6	Подстановоные и перестановочные преобразования в симметричных шифрах	Моноалфавитная подстановка. Полиалфавитная подстановка. Омофоническая и полиграммная подстановки. Простая перестановка. Маршрутная перестановка. Табличная перестановка.
7	Поточные шифры	Основы поточного шифрования. Синхронные и самосинхронизирующиеся поточные шифры. Генераторы псевдослучайных числовых последовательностей на основе регистров сдвига с линейной обратной связью.

8	Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Магма».	Требования к современным композиционным симметричным шифрам. Сеть Фейстеля. Примитивные операции, используемые при построении блочных алгоритмов. Шифр «Магма» как частный случай сети Фейстеля.
9	Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Кузнечик»	Виды преобразования информации в шифре «Кузнечик». LSX-преобразование. Базовые алгоритмы зашифрования и расшифрования в шифре «Кузнечик». Процедура получения раундовых подключей в шифре «Кузнечик».
10	Режимы использования современных композиционных шифров. Стандарт ГОСТ Р 34.13-2015	Использование блочных шифров в режиме простой. 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.
11	Асимметричные криптосистемы. Протоколы шифрования с открытым ключом и защищенной передачи ключей	Принципы построения и функционирования асимметричных криптосистем. Классификация асимметричных криптосистем. Криптосистема RSA. Протокол получения общего секретного ключа Диффи-Хеллмана. Протокол открытого шифрования Эль-Гамаля. Протокол «бесключевого шифрования» Месси-Омуры.
12	Схемы ЭЦП на основе вычислений по RSA-модулю и в конечном поле	Понятие электронной цифровой подписи (ЭЦП). Требования к ЭЦП. Использование криптографических хеш-функций в схемах ЭЦП. Требования, предъявляемые к хэш-функциям. Типовые схемы вычисления хеш-функций. Схема ЭЦП Ривеста-Шамира-Адлемана (RSA). Схема ЭЦП Рабина. Системы ЭЦП на основе задачи дискретного логарифмирования в конечном поле: схема Эль-Гамаля, схема DSA.
13	Схема ЭЦП на основе вычислений в группе точек эллиптической кривой	Математические основы эллиптической криптографии. Схемы формирования и проверки ЭЦП на основе ГОСТ Р 34.10-2012.

14	Инфраструктура открытых ключей	Сертификат ключа. Понятие инфраструктуры открытых ключей. Верификация цепочки сертификатов. Стандарты в области инфраструктуры открытых ключей.
15	Защита от несанкционированного доступа (НСД) в автоматизированных и управляющих информационных систем (АИУС)	Защита от НСД: основные термины и определения. Способы идентификации и аутентификации субъектов в АИУС. Дискреционная модель управления доступом в АИС. Ролевая модель управления доступом в АИС. Мандатная модель управления доступом в АИС.
16	Методы и механизмы обеспечения информационной безопасности в системах баз данных	Механизмы управления изолированностью транзакций в системах баз данных. Механизмы управления доступом в СУБД. Применение криптографических методов защиты информации в СУБД. Средства шифрования и резервирования в СУБД.
17	Безопасность компьютерных сетей	Назначение и функции межсетевых экранов. Использование межсетевых экранов для построения «демилитаризованных зон». Классификация межсетевых экранов. Виртуальные защищенные сети.
18	Защита от разрушающих программных воздействий	Понятие разрушающего программного воздействия (РПВ). Классификация вредоносного программного обеспечения. Методы и средства антивирусной защиты. Методы и средства выявления программных закладок. Запуск доверенных приложений под политикой безопасности.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	2	3	4	5	6
1	Введение в дисциплину	1	-	-	4
2	Угрозы информационной безопасности и уязвимости автоматизированных информационных систем	2	-	-	4
3	Общая характеристика и классификация методов защиты информации	2	-	-	4
4	Введение в криптографию	2	-	4	4
5	Модель и математические	2	-	4	4

	характеристики симметричных шифров				
6	Простейшие симметричные шифры	2	-	4	4
7	Поточные шифры	2	-	4	4
8	Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Магма».	2	-	-	4
9	Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Кузнечик»	2	-	-	4
10	Режимы использования современных композиционных шифров. Стандарт ГОСТ Р 34.13-2015	2	-	-	4
11	Асимметричные криптосистемы. Протоколы шифрования с открытым ключом и защищенной передачи ключей	2	-	6	4
12	Схемы ЭЦП на основе вычислений по RSA-модулю и в конечном поле	2	-	4	4
13	Схема ЭЦП на основе вычислений в группе точек эллиптической кривой	2	-	-	4
14	Инфраструктура открытых ключей	2	-	2	4
15	Защита от несанкционированного доступа (НСД) в автоматизированных и управляющих информационных систем (АИУС)	2	-	4	4
16	Методы и механизмы обеспечения информационной безопасности в системах баз данных	1	-	-	4
17	Безопасность компьютерных сетей	1	-	-	3,5
18	Защита от разрушающих программных воздействий	1	-	-	3,5
Итого		32	-	32	71

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

№ п/п	Наименование раздела	Перечень учебно-методического обеспечения
1	Введение в дисциплину	Основная литература: [1] Дополнительная литература: [1]
2	Угрозы информационной безопасности и уязвимости автоматизированных информационных систем	
3	Общая характеристика и классификация методов защиты информации	
4	Введение в криптографию	
5	Модель и математические характеристики симметричных шифров	
6	Простейшие симметричные шифры	
7	Поточные шифры	
8	Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015: шифр «Магма».	Нормативно-правовая документация: [3]
9	Отечественный стандарт	

	блочного шифрования ГОСТ Р 34.12-2015: шифр «Кузнечик»	
10	Режимы использования современных композиционных шифров. Стандарт ГОСТ Р 34.13-2015	Нормативно-правовая документация: [4]
11	Асимметричные криптосистемы. Протоколы шифрования с открытым ключом и защищенной передачи ключей	Основная литература: [1] Дополнительная литература: [1], [2]
12	Схемы ЭЦП на основе вычислений по RSA-модулю и в конечном поле	
13	Схема ЭЦП на основе вычислений в группе точек эллиптической кривой	Основная литература: [1] Дополнительная литература: [1], [2] Нормативно-правовая документация: [1], [2]
14	Инфраструктура открытых ключей	Основная литература: [1], [2] Дополнительная литература: [1], [2]
15	Защита от несанкционированного доступа (НСД) в автоматизированных и управляющих информационных систем (АИУС)	
16	Методы и	

	механизмы обеспечения информационной безопасности в системах баз данных	
17	Безопасность компьютерных сетей	
18	Защита от разрушающих программных воздействий	

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: 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.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. 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.

2. 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.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

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

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

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

4. 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

При освоении данной дисциплины другие издания не используются

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 данному направлению 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 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
«19» апреля 2018 г. М. Л. Глухарев