

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Кафедра «Информатики и информационной безопасности»

РАБОЧАЯ ПРОГРАММА

дисциплины

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ» (Б1.В.ОД.3)**

для специальности

23.05.04 «Эксплуатация железных дорог»

по специализации:

«Магистральный транспорт»

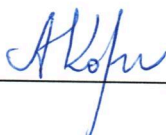
Форма обучения – очная, заочная

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
«25» 04 2018 г.


_____ А.Г. Котенко

Председатель учебно-методической комиссии
факультета «Управление перевозками и
логистика»

«25» апреля 2018 г.


_____ Т.Г. Сергеева

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 17.10.2016 № 1289 по специальности 23.05.04 «Эксплуатация железных дорог» по дисциплине «Информационная безопасность и защита информации на железнодорожном транспорте».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других дисциплин вариативной части Блока 1 в соответствии с требованиями, установленными федеральным государственным образовательным стандартом (приказ Минобрнауки России от 17.10.2016 № 1289) для формирования у выпускника общепрофессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: производственно-технологической; организационно-управленческой; проектной; научно-исследовательской и специализацией «Магистральный транспорт».

Для достижения цели поставлены задачи ведения дисциплины:

- подготовка обучающегося по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
- подготовка обучающегося к освоению дисциплины «Информационные технологии в грузовой и коммерческой работе» (Б1.Б.48);
- развитие социально-воспитательного компонента учебного процесса;
- изучение основных понятий в области информационной безопасности;
- изучение основ обеспечения информационной безопасности (в т.ч. на ж/д транспорте);
- изучение содержания организационных методов защиты информации (в т.ч. на ж/д транспорте);
- изучение содержания правовых методов защиты информации (в т.ч. на ж/д транспорте);
- изучение содержания технических методов защиты информации (в т.ч. на ж/д транспорте).

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 понятия в области обеспечения информационной безопасности;
- основные положения нормативных актов по защите информации;

– порядок сертификации средств защиты информации и лицензирования деятельности по защите информации;

– порядок и содержание правовых, организационных и технических мер по обеспечению информационной безопасности на железнодорожном транспорте.

УМЕТЬ:

– основные понятия в области обеспечения информационной безопасности;

– основные положения нормативных актов по защите информации;

– порядок сертификации средств защиты информации и лицензирования деятельности по защите информации;

– порядок и содержание правовых, организационных и технических мер по обеспечению информационной безопасности на железнодорожном транспорте.

ВЛАДЕТЬ:

– технологией построения моделей угроз информационных систем;

– методологией создания комплексных систем информационной безопасности;

– методами и средствами защиты информации.

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

– способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, готовностью соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны и коммерческих интересов (ОПК-4);

– владением основными методами, способами и средствами получения, хранения и переработки информации, наличием навыков работы с компьютером как средством управления информацией и автоматизированными системами управления базами данных (ОПК-5);

профессиональных компетенций (ПК):

– готовностью к эксплуатации автоматизированных систем управления поездной и маневровой работой, использованию информационных систем мониторинга и учета выполнения технологических операций (ПК-12);

профессионально-специализированных компетенций (ПСК):

– готовностью к применению информационных технологий на всех уровнях управления эксплуатационной работой магистрального железнодорожного транспорта, пользованию компьютерными базами данных, информационно-телекоммуникационной сетью "Интернет" (далее – сеть "Интернет"), средствами автоматизации управленческого труда и защиты информации, использованию технических средств производства переработки информации - аппаратного, математического и программного обеспечения (ПСК-1.2).

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

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

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность и защита информации на железнодорожном транспорте» (Б1.В.ОД.3) относится к вариативной части и является обязательной дисциплиной для обучающегося.

4. Объем дисциплины и виды учебной работы

Для очной формы обучения:

Вид учебной работы	Всего часов	Семестр
		VI
Контактная работа (по видам учебных занятий)	32	32
В том числе:		
– лекции (Л)	16	16
– практические занятия (ПЗ)	16	16
– лабораторные работы (ЛР)	-	-
Самостоятельная работа (СРС) (всего)	31	31
Контроль	9	9
Форма контроля знаний	зачет	зачет
Общая трудоемкость: час / з.е.	72/2	72/2

Для заочной формы обучения:

Вид учебной работы	Всего часов	Курс
		III
Контактная работа (по видам учебных занятий)	8	8
В том числе:		
– лекции (Л)	4	4
– практические занятия (ПЗ)	4	4
– лабораторные работы (ЛР)	-	-
Самостоятельная работа (СРС) (всего)	60	60
Контроль	4	4
Форма контроля знаний	зачет	зачет
Общая трудоемкость: час / з.е.	72/2	72/2

5. Содержание и структура дисциплины

5.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Введение	Информация. Классификация информации по категориям доступа. Свойства информации. Угрозы информационной безопасности. Уязвимости информационных систем. Способы защиты информации. Средства защиты информационных систем. Доктрина информационной безопасности.
2	Государственная система защиты информации в Российской Федерации	Организационная структура государственной системы защиты информации в Российской Федерации (ОАО РЖД). Функции и задачи Федеральной службы по техническому и экспортному контролю. Информационная безопасность в системе национальной безопасности. Система сертификации средств защиты информации. Система лицензирования деятельности в области защиты информации. Обзор и краткое содержание законов и национальных стандартов Российской Федерации и международных стандартов в области информационной безопасности.
3	Угрозы информационной безопасности на железнодорожном транспорте	Активы организации. Источники угроз. Классификация угроз. Модель нарушителя информационной безопасности. Правила разграничения доступа к ресурсам системы. Управление информационной безопасностью в ОАО РЖД. Меры по обеспечению безопасности в государственных информационных системах
4	Менеджмент информационной безопасности	Политика безопасности. Порядок разработки политики безопасности. Реализация политики безопасности. Пересмотр политики безопасности. Построение модели угроз информационной безопасности объекта информатизации. Меры по обеспечению безопасности государственных информационных систем. Категорирование, аттестация объектов информатизации. Классификация информационных систем. Разработка организационно-распорядительных документов по защите информации.

5.2 Разделы дисциплины и виды занятий
Для очной формы обучения:

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Введение	4	4	-	7
2	Государственная система защиты информации в Российской Федерации	4	4	-	8
3	Угрозы информационной безопасности на железнодорожном транспорте	4	4	-	8
4	Менеджмент информационной безопасности	4	4	-	8
Итого		16	16	-	31

Для заочной формы обучения:

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Введение	1	1	-	15
2	Государственная система защиты информации в Российской Федерации	1	1	-	15
3	Угрозы информационной безопасности на железнодорожном транспорте	1	1	-	15
4	Менеджмент информационной безопасности	1	1	-	15
Итого		4	4	-	60

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

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1	Введение	Система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_156018/ Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3Q6X8uNTJ
2	Государственная система защиты информации в Российской Федерации	
3	Угрозы информационной безопасности на железнодорожном транспорте	Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: http://fstec.ru/
4	Менеджмент информационной безопасности	

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. Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] : Учебные пособия – Электрон. дан. – М.: ДМК Пресс, 2014. – 702 с.;

2. 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]: Учебники — Электрон. дан. — М.: УМЦ ЖДТ, 2014. — 440 с.;

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Иванова Н.В., Коробулина О.Ю. Аудит информационной безопасности. – СПб.: ПГУПС, 2011. – 40 с.

2. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью. – СПб.: ПГУПС, 2010. – 44 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Технический регламент о требованиях пожарной безопасности: № 123-ФЗ от 22 июля 2008 г. // Российская газета / Уч-ль : Правительство РФ. - М. : Российская газета, 2008. - N163: 1 августа. - С. 18-24.

2. Стратегия национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Российская газета / Уч-ль : Правительство РФ. - М. : Российская газета, 2015. – N364: 31 декабря. - С. 22-23.

3. Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646 // Российская газета / Уч-ль : Правительство РФ. - М. : Российская газета, 2015. – N344: 5 декабря. - С. 22-25.

8.4 Другие издания, необходимые для освоения дисциплины

1. В.А. Кулишкин Аттестация объектов информатизации по требованиям безопасности конфиденциальной информации: Учебное пособие (Методические указания по выполнению лабораторных работ). – СПб.: ПГУПС, 2006, 40 с.;

2. В.А. Кулишкин Организационное обеспечение информационной безопасности: Методические указания для выполнения лабораторных работ. – СПб.: ПГУПС, 2009, 87 с.;

3. В.А. Кулишкин Разработка организационно-распорядительных документов: Учебное пособие (Методические указания по выполнению лабораторных работ). – СПб.: ПГУПС, 2010, 65 с.;

4. В.А. Кулишкин Разработка должностных инструкций: Учебное пособие. – СПб.: ПГУПС, 2014, 100 с. Электронный вариант. База данных менеджмент образовательного процесса на кафедре;

5. В.А. Кулишкин Деловая игра «Аттестация объектов информатизации»: Учебное пособие. – СПб.: ПГУПС, 2012, 29 с.

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

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (<http://fstec.ru/>);

2. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: (<http://tk.gost.ru/wps/portal/tk362>);

3. Электронный фонд нормативно-правовой документации. [Электронный ресурс] - Режим доступа: (<http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype>);

4. Система ГАРАНТ: <http://base.garant.ru/12148555/#ixzz3Q6X8uNTJ>;

5. Интернет-университет информационных технологий.
<http://www.intuit.ru>

6. Проект «Информационная безопасность и защита информации».
<http://www.itsec.ru/>

7. Интернет-версия системы «Консультант-Плюс».
<http://www.consultant.ru/>

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

9. Электронно-библиотечная система ЛАНЬ [Электронный ресурс]. Режим доступа: <https://e.lanbook.com> — Загл. с экрана.

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.

– электронная информационно-образовательная среда Петербургского государственного университета путей сообщения Императора Александра I [Электронный ресурс]. – Режим доступа: <http://sdo/pgups.ru>.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

– Microsoft Windows 7;

– Office Standard 2010 Russian OpenLicensePack NoLevel AcademicEdition;

– Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://get.adobe.com/ru/reader/>);

– Visual Studio Professional 2010 Russian OLP NL AcademicEdition;

– 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 информационной безопасности информационно-коммуникационных систем (ауд. 2-104), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; 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



А.М. Перепеченов

«24» апреля 2018 г.