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

«РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЁННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ» (Б1.Б.18)

для направления/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 «1» декабря 2016г., приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем», по дисциплине «Разработка и эксплуатация защищённых автоматизированных систем» (Б1.Б.18).

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе базовой части дисциплин в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектно-конструкторская, контрольно-аналитическая, организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели решаются следующие задачи:

- знакомство с основными нормативно-правовыми актами международного, федерального и ведомственного уровня, определяющими организационные и методические аспекты в области надежности защищённых автоматизированных систем (АС ЗИ);

- изучение основ теории надежности технических систем;

- изучение методологии анализа и обеспечения надежности АС и СЗИ на этапах проектирования, испытаний и эксплуатации;
- изучение современных методов и программных средств проектной оценки надежности структурно-сложных систем.

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 нормативные документы и стандарты в области разработки автоматизированных систем в защищенном исполнении;
- порядок и содержание стадий и этапов создания автоматизированных систем в защищенном исполнении;
- основные нормативные документы и стандарты в области эксплуатации автоматизированных систем в защищенном

исполнении;

УМЕТЬ:

- формировать требования к подсистемам информационной безопасности автоматизированных систем в защищенном исполнении;
- осуществлять и обосновывать выбор элементной базы и средств защиты для автоматизированных систем в защищенном исполнении;
- оценивать показатели риска автоматизированных систем в защищенном исполнении на этапах проектирования, испытаний и эксплуатации;
- контролировать эффективность проектирования, разработки, внедрения и эксплуатации автоматизированных систем в защищенном исполнении;

ВЛАДЕТЬ:

- методами проектирования систем, удовлетворяющих заданным требованиям надежности и информационной безопасности;

- методиками оценки показателей качества и эффективности автоматизированных систем;

- навыками участия в экспертизе состояния защищенности информации на объекте защиты.

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 **профессиональных компетенций (ПК)**, соответствующих виду профессиональной деятельности, на который ориентирована программа:

научно-исследовательская деятельность:

способностью создавать и исследовать модели автоматизированных систем (ПК-2);

способностью проводить анализ защищенности автоматизированных систем (ПК-3);

проектно-конструкторская деятельность:

способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-8);

контрольно-аналитическая:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-15);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

организационно-управленческая:

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

эксплуатационная деятельность:

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25).

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 «Разработка и эксплуатация защищённых автоматизированных систем» (Б1.Б.18) относится к базовой части и является обязательной для обучающегося.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр	
		8	9
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	64 32 - 32	32 16 - 16	32 16 - 16
Самостоятельная работа (СРС) (всего)	71	31	40
Контроль	45	9	36
Форма контроля знаний		З	Э
Общая трудоемкость: час / з.е.	180/5	72/2	108/3

5. Содержание и структура дисциплины

5.1 Содержание дисциплины

№ П/П	Наименование раздела дисциплины	Содержание раздела
1	Введение в дисциплину	Предмет и задачи дисциплины. Рекомендуемая литература и указания по самостоятельной работе. Краткая историческая справка о развитии информационной безопасности. Научные основы дисциплины в системе подготовки специалистов в области АС и СЗИ. Основные понятия и определения, используемые в рамках дисциплины.
2	Разработка защищенных автоматизированных систем	Система стандартов в области разработки АС и АСЗИ. Национальные, межгосударственные и международные стандарты в области защиты информации. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Основные стадии и этапы создания АС. Модель проектирования АСЗИ. Принципы организации и структура систем защиты автоматизированных систем. Особенности разработки технического задания на создание подсистем информационной безопасности автоматизированных систем. Методы обоснования структурного состава АСЗИ.
3	Модели угроз	Понятие модели угроз. Нормативные документы ФСТЭК, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Принципы формирования политики информационной безопасности в АС. Практические подходы к разработке моделей угроз. Типовые структуры автоматизированных систем и модели угрозы. Критерии и классы защищенности автоматизированных систем.
4	Модели нарушителей	Понятие модели угроз. Нормативные документы ФСТЭК, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Принципы формирования политики информационной безопасности в АС. Практические подходы к разработке моделей угроз. Типовые структуры автоматизированных систем и модели нарушителей

5	Методы анализа риска и информационной безопасности в автоматизированных системах	Методы анализа структурных и функциональных схем защищенных автоматизированных информационных систем. Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем. Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы.
6	Система эксплуатации защищенных автоматизированных систем	Содержание и методы риск-ориентированного подхода к анализу эксплуатации АС и СЗИ. Жизненный цикл АС и СЗИ. Концепция УРРАН. Задачи и структура информационных технологий комплексного управления эксплуатацией АС. Основные определения и понятия системы эксплуатации АС и СЗИ.
7	Система технической эксплуатации защищенных автоматизированных систем	Основные определения и понятия технической эксплуатации АС и СЗИ. Содержание эксплуатационной документации автоматизированной системы. Методы анализа функциональной безопасности автоматизированных систем. Особенности эксплуатации комплексных систем обеспечения информационной безопасности на объекте защиты. Реализация систем контроля доступа. Способы представления информации о правах доступа.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1.	Введение в дисциплину	2	-	-	2
2.	Разработка защищенных автоматизированных систем	6	-	4	6
3.	Модели угроз	4	-	4	8
4	Модели нарушителей	4	-	4	8
5	Методы анализа риска и информационной безопасности в	6	-	8	7

	автоматизированных системах				
6	Система эксплуатации защищенных автоматизированных систем	6	-	6	20
7	Система технической эксплуатации защищенных автоматизированных систем	4	-	6	20
Итого		32	-	32	71

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

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1.	Введение в дисциплину	Перепечёнов А.М. Основы проектирования защищенных информационных систем/ А.М. Перепечёнов. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2013. -59с.
2.	Разработка защищенных автоматизированных систем	
3.	Модели угроз	Корниенко А.А. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте/ А.А.Корниенко и др. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2016. -45с.
4	Модели нарушителей	
5	Методы анализа риска и информационной безопасности в автоматизированных системах	Ветлугин К.А. Алгоритмы автоматизированного структурно-логического моделирования надежности и безопасности информационных и телекоммуникационных систем. Учебное пособие. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2016. – 47с
6	Система эксплуатации защищенных автоматизированных систем	Половко А.М., Гуров С.М. Основы теории надежности. BHV – Санкт-Петербург, 2009. – 560с.
7	Система технической эксплуатации защищенных автоматизированных систем	

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. Корниенко А.А. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте/ А.А.Корниенко и др. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2016. -45с.
2. Перепечёнов А.М. Основы проектирования защищенных информационных систем/ А.М. Перепечёнов. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2013. -59с.
3. Ветлугин К.А. Алгоритмы автоматизированного структурно-логического моделирования надежности и безопасности информационных и телекоммуникационных систем. Учебное пособие./ К.А. Ветлугин, А.В.Струков. ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2016. – 47с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Коцюба И.Ю.Основы проектирования информационных систем. Учебное пособие/ И.Ю. Коцюба, А.В.Чунаев, А.Н.Шиков. Университет ИТМО. – Санкт-Петербург. 2015. -206с.
2. Половко А.М., Гуров С.М. Основы теории надежности. BHV – Санкт-Петербург, 2009. – 560с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность, и обозначения документов при создании автоматизированных систем.
2. ГОСТ 34.601-89. Информационная технология. Комплекс стандартов на автоматизированные системы.

3. ГОСТ Р 51583-2014. Защита информации. Порядок создания АС в защищенном исполнении.

8.4 Другие издания, необходимые для освоения дисциплины

Корниенко А.А., Нозик А.А., Струков А.В. Моделирование и автоматизированный расчет надежности информационных систем и средств защиты информации. Учебное пособие. – СПб.:ПГУПС, 2014, 33с.

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;
- 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.

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 А.В.Струков
«24» 04 2018 г.