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»

ПРОГРАММА

производственной практики
«ПРЕДДИПЛОМНАЯ ПРАКТИКА» (Б2.П.3)

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

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

Заведующий кафедрой
Информатика и информационная
безопасность

« » 2018 г. _____ А.А. Корниенко

СОГЛАСОВАНО

Руководитель ОПОП

« » 2018 г. _____ А.А. Корниенко

Председатель методической комиссии
факультета «Автоматизация и
интеллектуальные технологии»

« » 2018 г. _____ М.Л. Глухарев

1. Вид практики, способы и формы ее проведения

Программа составлена в соответствии с ФГОС ВО, утвержденным «01» декабря 2016 г., приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем», по производственной практике «Преддипломная практика».

Вид практики – производственная, в соответствии с учебным планом подготовки специалиста, утвержденным «21» февраля 2017 г.

Тип практики: преддипломная практика.

Проводится для выполнения выпускной квалификационной работы.

Способ проведения практики – стационарная.

Практика проводится дискретно по видам практик.

Практика проводится в следующей форме: путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждого вида (совокупности видов) практики.

Практика проводится на кафедре «Информатика и информационная безопасность» ПГУПС.

Задачей преддипломной практики и реального дипломного проектирования по заявкам предприятий является обобщение, систематизация и совершенствование знаний и умений обучающихся по будущей профессии, подготовка материалов к выпускной квалификационной работе.

2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемыми результатами прохождения практики является приобретение знаний, умений, навыков и/или опыта деятельности.

В результате прохождения практики обучающийся должен:

ЗНАТЬ:

– систему компьютерной и информационной безопасности подразделения и систему противодействия техническим разведкам;

– организацию научной, изобретательской и рационализаторской работы, проводимой подразделением в интересах совершенствования выполнения служебных задач;

– процесс проектирования, производства и эксплуатации средств компьютерной и информационной безопасности;

– организацию служебной и производственной деятельности подразделения;

– структурные и функциональные схемы, используемые в подразделениях компьютерной и информационной безопасности;

– порядок и методы проведения планово-профилактических и ремонтно-восстановительных работ;

– характеристики и возможности диагностического оборудования и измерительных приборов, входящих в состав рабочих мест;

– характеристики технических средств, используемых при разработке, изготовлении и эксплуатации средств компьютерной, информационной безопасности и противодействия техническим разведкам;

– современные методы и средства разработки и оценки модели и политики безопасности.

УМЕТЬ:

– выполнять основные функциональные обязанности в соответствии с должностью;

– работать с технической и эксплуатационной документацией;

– использовать современные средства разработки программного обеспечения на языках высокого уровня и языках СУБД, библиотеки объектов и классов для решения задач создания и сопровождения автоматизированных систем;

– применять стандартные криптографические решения для защиты информации и квалифицированно оценивать их качество;

– реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

– выполнять функциональные обязанности в соответствии с должностью специалиста (инженера) по защите информации;

– проводить планово-профилактические и ремонтные работы;

– вести учетно-отчетную документацию;

– проводить занятия с техническим персоналом подразделения;

– выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации;

– решать задачи защиты программ и данных программно-аппаратными средствами и оценивать качество предлагаемых решений.

ВЛАДЕТЬ:

– методами системного подхода к обеспечению информационной безопасности в различных сферах деятельности подразделения.

– методами планирования и проведения специальных технических мероприятий, направленных на повышение эффективности функционирования системы компьютерной и информационной безопасности подразделения;

– используемыми в подразделении методами определения и измерения параметров опасных сигналов для технических каналов утечки информации;

– методами анализа используемых в подразделении технологий обработки данных в распределенных системах с целью оптимизации их производительности и повышения надежности функционирования.

ОПЫТ ДЕЯТЕЛЬНОСТИ:

- опыт научно-исследовательской деятельности;
- опыт проектно-конструкторской деятельности;
- опыт контрольно-аналитической деятельности;
- опыт организационно-управленческой деятельности;
- опыт эксплуатационной деятельности.

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

Прохождение практики направлено на формирование следующих **общекультурных компетенций (ОК)**:

- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7).

Прохождение практики направлено на формирование следующих **общепрофессиональных компетенций (ОПК)**:

- способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7).

Прохождение практики направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих виду профессиональной деятельности, на который ориентирована программа специалитета:

Научно-исследовательская:

- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
- способностью создавать и исследовать модели автоматизированных систем (ПК-2);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7).

Проектно-конструкторская:

- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13).

Контрольно-аналитическая:

- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17).

Организационно-управленческая:

- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23).

Эксплуатационная:

- способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
- способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);
- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Прохождение практики направлено на формирование следующих **профессионально-специализированных компетенций (ПСК)**, соответствующих специализации программы специалитета:

- способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1);
- способностью разрабатывать политику безопасности для совершенствования системы управления информационной безопасностью распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.2);
- способностью осуществлять рациональный выбор средств и разрабатывать предложения по обеспечению информационной безопасности распределенных

автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.3);
- способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-10.4);
- способностью обеспечить эффективное применение средств защиты электронного технологического документооборота и технического документоведения на транспорте (по видам) (ПСК-10.5).

Область профессиональной деятельности обучающихся, прошедших данную практику, приведена в п. 2.1 ОПОП.

Объекты профессиональной деятельности обучающихся, прошедших данную практику, приведены в п. 2.2 ОПОП.

3. Место практики в структуре основной профессиональной образовательной программы

Практика «Преддипломная практика» (Б2.П.3) относится к Блоку 2 «Практики, в том числе научно-исследовательская работа (НИР)» и является обязательной.

4. Объем практики и ее продолжительность

Практика распределена в течение учебного семестра.

Вид учебной работы	Всего часов	Семестр 10
Форма контроля знаний	З	З
Общая трудоемкость: час / з.е.	648/18	648/18
Продолжительность практики: неделя	12	12

5. Содержание практики

Первая неделя: Получение темы и состава ВКР и исходных данных. Изучение учебной и нормативной литературы по теме ВКР

Вторая и третья неделя: Изучение и обобщение опыта работы и материалов предприятия по теме ВКР

Четвертая – одиннадцатая недели: Проработка принципиальных технических решений по разделам ВКР.

Двеннадцатая неделя: Написание отчета по практике

6. Формы отчетности

По итогам практики обучающимся составляется отчет с учетом индивидуального задания, выданного руководителем практики от Университета.

Структура отчета по практике представлена в фонде оценочных средств.

После прибытия на предприятие и оформления направления на практику в отделе кадров (отделе управления персоналом), обучающийся направляет в электронном виде отсканированное направление на практику с отметкой о прибытии в адрес руководителя по практике кафедры, ответственного за организацию практики. После завершения практики предприятие ставит отметку об убытии с практики в направлении на практику.

Направление на практику с отметками предприятия о прибытии и убытии обучающегося на практику сдается на кафедру, ответственную за организацию практики.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Фонд оценочных средств по практике является неотъемлемой частью программы практики 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 проведения практики

8.1 Перечень основной учебной литературы, необходимой для прохождения практики

1. А.А. Малюк, В.С. Горбатов, В.И. Королев и др. Введение в информационную безопасность: Учебное пособие для вузов. М.: Научно-техническое издательство «Горячая линия – Телеком», 2014. 288 с.

2. В.А. Тихонов, В.В. Райх Информационная безопасность: концептуальные , правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с., ил.

3. С.Н. Семкин, А.Н. Семкин Основы правового обеспечения защиты информации: Учебное пособие для ВУЗов. - М.: Горячая линия-Телеком, 2010. М.: «Гелиос-АРВ», 2010. -239 с.: ил.

8.2 Перечень дополнительной учебной литературы, необходимой для прохождения практики

1. Конституция Российской Федерации. // Российская газета № 7 от 22.12.2008г.

2. Концепция национальной безопасности Российской Федерации. // Российская газета от 26.12.1997г.

3. Доктрина информационной безопасности Российской Федерации. // Российская газета от 10.09.2000г.
4. В.А. Кулишкин Краткий курс лекций по дисциплине «Основы информационной безопасности»: Учебное пособие. – СПб.: ПГУПС, 2008.-232 с.

8.3 Перечень нормативно-правовой документации, необходимой для прохождения практики

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3Q6X8uNTJ
2. Закон РФ от 21.07.1993 N 5485-1 (ред. от 21.12.2013) "О государственной тайне" (21 июля 1993 г.) Система Консультант Плюс http://www.consultant.ru/document/cons_doc_LAW_156018/

8.4 Другие издания, необходимые для прохождения практики

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 прохождения практики

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (http://fstec.ru/);
2. 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;
3. Официальный сайт информационной сети ТЕХЭКСПЕРТ [Электронный ресурс] - Режим доступа: *http://www.cntd.ru/*, свободный;

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

5. Информационно-поисковая система «МИМОЗА» (База данных о изобретениях и полезных моделях с 1994 г. по н.в.) (Установлена на компьютере преподавателя в ауд. 2/110);

6. База данных «Система ГОСТов по обеспечению информационной безопасности» (Свидетельство о государственной регистрации базы данных №2014621325 от 18.09.2014

10. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем

Системой информационного обеспечения практики предусматриваются использование единой автоматизированной информационной системы управления Университета (ЕАИСУ) для учета прохождения практики обучающимися с первого по пятый курсы.

Перечень информационных технологий, используемых при проведении практики:

- технические средства (компьютерная техника и средства связи (персональные компьютеры, интерактивная доска);
- методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов);
- перечень Интернет-сервисов и электронных ресурсов (поисковые системы, электронная почта, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники, электронные учебные и учебно-методические материалы)
- Протоколы – IP, SDH, PDH
- Протоколы безопасной передачи информации – IPSec, PPP, L2TP, SSL, TLS
- Технологии локальных вычислительных систем – Ethernet, Fast Ethernet
- Технологии сетей доступа – WiFi, WiMAX
- Технологии систем связи – GSM, CDMA, GPRS, ATM, Frame Relay
-Стандарты шифрования, криптографические системы и типовые криптографические схемы – DES, 3DES, AES, ГОСТ Р 34.10-2001, RSA, DH, ElGamal, Shnorr.

Кафедра «Информатика и информационная безопасность» обеспечена необходимым комплектом лицензионного программного обеспечения:

- Microsoft Windows 7;
- Microsoft Word 2010;
- Microsoft Excel 2010;
- Microsoft PowerPoint 2010.

10. Описание материально-технической базы, необходимой для проведения практики

- Общество с ограниченной ответственностью «Удостоверяющий центр ГАЗИНФОРМСЕРВИС» (ООО УЦ ГИС);
- Открытое акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ОАО «НИИАС»);
- Закрытое акционерное общество «АКУТА»;
-Закрытое Акционерное Общество «Ассоциация специалистов информационных систем»;
- Общество с ограниченной ответственностью «Научно-производственное предприятие «Специальные вычислительные комплексы» (ООО НПП «СВК»);
СПб ВЦ структурное подразделение ГВЦ филиала ОАО РЖД

Разработчик программы,
старший преподаватель
«23» апреля 2018 года О.В. Петрова