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

Б2.П.В.1 «ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА»

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на железнодорожном транспорте*»

Форма обучения – очная

Санкт-Петербург
2025

ЛИСТ СОГЛАСОВАНИЙ

Программа рассмотрена и утверждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 10 от 31 марта 2025 г.

И.о. заведующего кафедрой
«Информатика и информационная безопасность»
31 марта 2025 г. К.З. Билятдинов

СОГЛАСОВАНО

Руководитель ОПОП
31 марта 2025 г. М.Л. Глухарев

1. Вид практики, способы и формы ее проведения

Программа практики «*Эксплуатационная практика»* составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению специальности *10.05.03* «*Информационная безопасность автоматизированных систем*» (далее – ФГОС ВО), утвержденного 26 ноября 2020 г., приказ Министерства науки и высшего образования Российской Федерации № 1457, с учетом профессионального стандарта *06.033 «Специалист по защите информации в автоматизированных системах»*, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н.

Вид практики – производственная практика.

Тип практики – эксплуатационная практика.

Способ проведения практики – стационарная.

Практика проводится дискретно по видам практик.

Практическая подготовка может быть организована как непосредственно в Университете, так и в профильных организациях, руководствующихся в своей деятельности профессиональным стандартом *06.033 «Специалист по защите информации в автоматизированных системах»*, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н.

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

Проведение практики направлено на практическую подготовку обучающегося к будущей профессиональной деятельности. Практическая подготовка осуществляется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенции (части компетенций) по профилю образовательной программы.

Сформированность компетенций (части компетенции) оценивается с помощью индикаторов достижения компетенций.

Индикаторы достижения компетенций	**Результаты прохождения практики**
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	
ОПК-1.1.3. Знает угрозы и источники угроз информационной безопасности современного общества	*Обучающийся знает:* – основные угрозы и источники угроз информационной безопасности современного общества
ОПК-1.1.4. Знает основные методы обеспечения информационной безопасности	*Обучающийся знает:* – основные методы обеспечения информационной безопасности
ПК-1. Тестирование систем защиты информации автоматизированных систем	
ПК-1.1.5. Знает технические средства контроля эффективности мер защиты информации	*Обучающийся знает:* – основные технические и программные средства защиты информации
ПК-1.2.3. Умеет контролировать	*Обучающийся умеет:*

Индикаторы достижения компетенций	Результаты прохождения практики
безотказное функционирование технических средств защиты информации	обеспечивать функционирование средств защиты информации
ПК-1.2.4. Умеет восстанавливать (заменять) отказавшие технические средства защиты информации	*Обучающийся умеет:* восстанавливать (заменять) средства защиты информации
ПК-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системах	*Обучающийся владеет:* Основами выявления угроз безопасности информации в автоматизированных системах

3. Место практики в структуре основной профессиональной образовательной программы

Практика «*Эксплуатационная практика*» (*Б2.В.01(П)*) относится к части, формируемой участниками образовательных отношений, Блока 2 «*Практика*» и является обязательной.

4. Объем практики и ее продолжительность

Практика проводится концентрировано.

Вид учебной работы	Всего	Семестр
		6
Общая трудоемкость: час / з.е.	216/6	216/6
В том числе, форма контроля знаний, час.	З/4	З/4
Продолжительность практики: недель	4	4

5. Содержание практики

Требования к содержанию практики, примерная тематика индивидуальных заданий представлены в Методических указаниях по прохождению практики.

6. Формы отчетности

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

Структура отчета по практике, требования к оформлению и процедуре защиты приведены в Методических указаниях по прохождению практики.

7. Оценочные материалы для проведения промежуточной аттестации обучающихся по практике

Оценочные материалы по практике являются неотъемлемой частью программы практики и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

8. Описание материально-технического и учебно-методического обеспечения, необходимого для реализации образовательной программы по практике

8.1. Материально-техническая база, необходимая для проведения практики, определяется в соответствии с индивидуальным заданием, с рабочим местом и видами работ, выполняемыми обучающимися в организации.

Для проведения текущего контроля и промежуточной аттестации по практике Университет имеет помещения, которые представляют собой учебные аудитории, укомплектованные специализированной учебной мебелью и оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории: настенным экраном (стационарным или переносным), маркерной доской и (или) меловой доской, мультимедийным проектором (стационарным или переносным).

Все помещения соответствуют действующим санитарным и противопожарным нормам и правилам.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

8.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

– MS Office;
– Операционная система Windows;
– Антивирус Касперский;
– Visual Studio Express (Visual Studio Community) – бесплатное, свободно распространяемое программное обеспечение, режим доступа https://visualstudio.microsoft.com/ru/vs/express/;
– Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/);
– Oracle Java SE Development Kit 8, в том числе встроенные в JRE криптографические сервис-провайдеры (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/);
– бесплатные, свободно распространяемые среды программ на языке Python (пакет Anaconda, режим доступа https://www.anaconda.com; Python IDLE, режим доступа https://www.python.org/).

8.4. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных:

– Электронно-библиотечная система издательства «Лань». [Электронный ресурс]. – URL: https://e.lanbook.com/ — Режим доступа: для авториз. пользователей;
– Электронно-библиотечная система ibooks.ru («Айбукс»). – URL: https:// ibooks.ru / — Режим доступа: для авториз. пользователей;
– Электронная библиотека ЮРАЙТ. – URL: https://biblio-online.ru/ — Режим доступа: для авториз. пользователей;
– Единое окно доступа к образовательным ресурсам - каталог образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования». – URL: http://window.edu.ru/ — Режим доступа: свободный.
– Словари и энциклопедии. – URL: http://academic.ru/ — Режим доступа: свободный.
– Научная электронная библиотека "КиберЛенинка" - это научная электронная библиотека, построенная на парадигме открытой науки (Open Science), основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии и повышение цитируемости российской науки.

– URL: http://cyberleninka.ru/ — Режим доступа: свободный;

– 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);

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

8.5. Перечень печатных и электронных изданий, используемых в образовательном процессе:

1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 440 с.

2. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 448 с.

3. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2016. – 45 с.

4. А. А. Корниенко, А. П. Глухов, С. В. Диасамидзе. Система предупреждения и обнаружения компьютерных атак (учебное пособие). - СПб.: ПГУПС, 2019. – 47 с.

5. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

6. Федеральные законы:

• «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006;

• «О коммерческой тайне» № 119-ФЗ от 29.07.2004;

• «О персональных данных» № 152-ФЗ от 27.07.2006.

7. Сборник Руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа – М: Гостехкомиссия, 1998. – 120 с.

8. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

9. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3.

10. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

11. ГОСТ ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

12. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

13. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

14. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.- М.: Стандартинформ, 2012. -12 с.

15. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

16. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

17. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

8.6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых в образовательном процессе:

1. Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://my.pgups.ru — Режим доступа: для авториз. пользователей;
2. Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://sdo.pgups.ru — Режим доступа: для авториз. пользователей;
3. Официальный портал Росстандарта http://www.gost.ru/wps/portal/, портал по стандартизации http://standard.gost.ru/wps/portal/
4. Официальный сайт ФСТЭК России http://www.fstec.ru/
5. Проект «Информационная безопасность». http://www.itsec.ru/
6. Проект «Национальный Открытый Университет «ИНТУИТ» http://www.intuit.ru/

Разработчик рабочей программы, *доцент* _____ *С.В. Корниенко*
31.03.2025