

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.3 «ПРЕДДИПЛОМНАЯ 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 «Преддипломная 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 – преддипломная 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, руководящихся 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
ПК-1. Тестирование систем защиты информации автоматизированных систем	
ПК-1.1.1. Знает принципы построения и функционирования систем и сетей передачи информации	<i>Обучающийся знает:</i> – принципы построения и функционирования систем и сетей передачи информации
ПК-1.1.2. Знает эталонную модель взаимодействия открытых систем	<i>Обучающийся знает:</i> – эталонную модель взаимодействия открытых систем
ПК-1.1.3. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	<i>Обучающийся знает:</i> – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
ПК-1.1.4. Знает основные меры по защите информации в	<i>Обучающийся знает:</i> – основные меры по защите информации в

Индикаторы достижения компетенций	Результаты прохождения практики
автоматизированных системах	автоматизированных системах
ПК-1.1.5. Знает технические средства контроля эффективности мер защиты информации	<p><i>Обучающийся знает:</i></p> <ul style="list-style-type: none"> – технические средства контроля эффективности мер защиты информации
ПК-1.2.1. Умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации
ПК-1.2.2. Умеет анализировать основные узлы и устройства современных автоматизированных систем	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – анализировать основные узлы и устройства современных автоматизированных систем
ПК-1.2.3. Умеет контролировать безотказное функционирование технических средств защиты информации	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – контролировать безотказное функционирование технических средств защиты информации
ПК-1.2.4. Умеет восстанавливать (заменять) отказавшие технические средства защиты информации	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – восстанавливать (заменять) отказавшие технические средства защиты информации
ПК-1.3.1. Имеет навыки проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-1.3.2. Имеет навыки выявления уязвимости информационно-технологических ресурсов автоматизированных систем	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – выявления уязвимости информационно-технологических ресурсов автоматизированных систем

Индикаторы достижения компетенций	Результаты прохождения практики
ПК-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системах	<i>Обучающийся имеет навыки:</i> – выявления основных угроз безопасности информации в автоматизированных системах
ПК-1.3.4. Имеет навыки составления методик тестирования систем защиты информации автоматизированных систем	<i>Обучающийся имеет навыки:</i> – составления методик тестирования систем защиты информации автоматизированных систем
ПК-1.3.5. Имеет навыки подбора инструментальных средств тестирования систем защиты информации автоматизированных систем	<i>Обучающийся имеет навыки:</i> – подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-1.3.6. Имеет навыки составления протоколов тестирования систем защиты информации автоматизированных систем	<i>Обучающийся имеет навыки:</i> – составления протоколов тестирования систем защиты информации автоматизированных систем
ПК-2. Разработка проектных решений по защите информации в автоматизированных системах	
ПК-2.1.1. Знает нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	<i>Обучающийся знает:</i> – нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
ПК-2.1.2. Знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов	<i>Обучающийся знает:</i> – принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов
ПК-2.1.3. Знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	<i>Обучающийся знает:</i> – критерии оценки эффективности и надежности средств защиты информации программного обеспечения
ПК-2.1.4. Знает принципы	<i>Обучающийся знает:</i>

Индикаторы достижения компетенций	Результаты прохождения практики
организации и структуру систем защиты информации программного обеспечения автоматизированных систем	– принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем
ПК-2.1.5. Знает принципы формирования политики информационной безопасности в автоматизированных системах	<i>Обучающийся знает:</i> – принципы формирования политики информационной безопасности в автоматизированных системах
ПК-2.2.1. Умеет применять нормативные документы по противодействию технической разведке	<i>Обучающийся умеет:</i> – применять нормативные документы по противодействию технической разведке
ПК-2.2.2. Умеет определять типы субъектов доступа и объектов доступа, являющихся объектами защиты	<i>Обучающийся умеет:</i> – определять типы субъектов доступа и объектов доступа, являющихся объектами защиты
ПК-2.2.3. Умеет определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	<i>Обучающийся умеет:</i> – определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе
ПК-2.2.4. Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах	<i>Обучающийся умеет:</i> – определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах
ПК-2.2.5. Умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	<i>Обучающийся умеет:</i> – определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-2.2.6. Умеет определять структуру системы защиты информации автоматизированной системы в соответствии с	<i>Обучающийся умеет:</i> – определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных

Индикаторы достижения компетенций	Результаты прохождения практики
требованиями нормативных правовых документов в области защиты информации автоматизированных систем	систем
ПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-2.3.2. Имеет навыки разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем
ПК-2.3.3. Имеет навыки разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-3. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	
ПК-3.1.1. Знает основные методы управления информационной безопасностью	<p><i>Обучающийся знает:</i></p> <ul style="list-style-type: none"> – основные методы управления информационной безопасностью
ПК-3.1.2. Знает информационные воздействия и критерии оценки защищенности автоматизированных систем	<p><i>Обучающийся знает:</i></p> <ul style="list-style-type: none"> – информационные воздействия и критерии оценки защищенности автоматизированных систем
ПК-3.1.3. Знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах	<p><i>Обучающийся знает:</i></p> <ul style="list-style-type: none"> – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах
ПК-3.1.4. Знает основные средства, способы и принципы построения систем защиты	<p><i>Обучающийся знает:</i></p> <ul style="list-style-type: none"> – основные средства, способы и принципы построения систем защиты информации

Индикаторы достижения компетенций	Результаты прохождения практики
информации автоматизированных систем	
ПК-3.2.1. Умеет проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов
ПК-3.2.2. Умеет разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных систем
ПК-3.2.3. Умеет исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных систем
ПК-3.2.4. Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем
ПК-3.2.5. Умеет оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите
ПК-3.2.6. Умеет исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности

Индикаторы достижения компетенций	Результаты прохождения практики
требуемого уровня защищенности	
ПК-3.2.7. Умеет проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации	<p><i>Обучающийся умеет:</i></p> <ul style="list-style-type: none"> – проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации
ПК-3.3.1. Имеет навыки анализа технической документации информационной инфраструктуры автоматизированной системы	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – анализа технической документации информационной инфраструктуры автоматизированной системы
ПК-3.3.2. Имеет навыки анализа защищенности информационной инфраструктуры автоматизированной системы	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – анализа защищенности информационной инфраструктуры автоматизированной системы
ПК-3.3.3. Имеет навыки формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач
ПК-3.3.4. Имеет навыки документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации
ПК-3.3.5. Имеет навыки обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	<p><i>Обучающийся имеет навыки:</i></p> <ul style="list-style-type: none"> – обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
ПК-4. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	

Индикаторы достижения компетенций	Результаты прохождения практики
ПК-4.1.1. Знает современные технологии программирования	<i>Обучающийся знает:</i> – современные технологии программирования
ПК-4.1.2. Знает основные протоколы локальных и глобальных сетей	<i>Обучающийся знает:</i> – основные протоколы локальных и глобальных сетей
ПК-4.1.3. Знает последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей	<i>Обучающийся знает:</i> – последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей
ПК-4.1.4. Знает принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения	<i>Обучающийся знает:</i> – принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения
ПК-4.1.5. Знает методы тестирования и отладки программного и аппаратного обеспечения	<i>Обучающийся знает:</i> – методы тестирования и отладки программного и аппаратного обеспечения
ПК-4.2.1. Умеет разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД	<i>Обучающийся умеет:</i> – разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД
ПК-4.3.1. Имеет навыки разработки технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты	<i>Обучающийся имеет навыки:</i> – разработки технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем

Индикаторы достижения компетенций	Результаты прохождения практики
автоматизированных систем	
ПК-4.3.2. Имеет навыки синтеза структурных и функциональных схем защищенных автоматизированных систем	<i>Обучающийся имеет навыки:</i> – синтеза структурных и функциональных схем защищенных автоматизированных систем
ПК-4.3.3. Имеет навыки разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации	<i>Обучающийся имеет навыки:</i> – разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации

3. Место практики в структуре основной профессиональной образовательной программы

Практика «Преддипломная практика» (Б2.В.03(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
		В
Общая трудоемкость: час / з.е.	756/21	756/21
В том числе, форма контроля знаний, час.	3/4	3/4
Продолжительность практики: недель	14	14

Примечание: «Форма контроля знаний» – экзамен (Э, 36 час.), зачет (З, 4 час.) – это примечание, как и все остальные, надо удалить перед распечаткой рабочей программы.

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. Обучающимся обеспечен доступ (удаленный доступ) к информационным справочным системам:

– Национальный Открытый Университет "ИНТУИТ". Бесплатное образование. [Электронный ресурс]. – URL: <https://intuit.ru/> — Режим доступа: свободный.

– Техническая документация по языку C++. [Электронный ресурс]. – URL: <https://docs.microsoft.com/> — Режим доступа: свободный.

– Техническая документация по языку программирования и платформе Java [Электронный ресурс] – Режим доступа: <https://docs.oracle.com/en/java/> (свободный доступ).

– Техническая документация по языку программирования Python [Электронный ресурс] – Режим доступа: <https://www.python.org/doc/> (свободный доступ).

8.6. Перечень печатных изданий, используемых в образовательном процессе:

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.

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

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

6. Доктрина информационной безопасности Российской Федерации. // Российская газета от 10.09.2000г.

7. В.А. Кулишкин. Краткий курс лекций по дисциплине «Основы информационной безопасности»: Учебное пособие. – СПб.: ПГУПС, 2008.-232 с.

8. 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>

9. 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/

8.7. 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
31.03.2025

С.В. Корниенко