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
Б1.В.6 «*РИСК-МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*»
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

Рабочая 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. Цели и задачи дисциплины

Рабочая программа дисциплины «*Риск-модели информационной безопасности» (Б1.В.06*) (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по 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.

Целью изучения дисциплины является расширение и углубление профессиональной подготовки для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности и специализацией «Информационная безопасность автоматизированных систем на транспорте»

Для достижения цели дисциплины решаются следующие задачи:

- изучение основных методов и подходов к повышению эффективности системы управления безопасностью информации в автоматизированных системах;
- изучение основных принципов и методов управления информационной безопасностью;
- анализ информационных активов автоматизированной системы с оцениванием их с точки зрения информационных рисков.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Планируемыми результатами обучения по дисциплине является формирование у обучающихся компетенций и/или части компетенций. Сформированность компетенций и/или части компетенций оценивается с помощью индикаторов достижения компетенций.

В рамках изучения дисциплины осуществляется практическая подготовка обучающихся к будущей профессиональной деятельности. Результатом обучения по дисциплине является формирования у обучающихся практических навыков.

- ПК-2.3.3. Имеет навыки разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ПК-2. Разработка проектных решений по защите информации в автоматизированных системах	
ПК-2.3.3. Имеет навыки разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	*Обучающийся владеет* основными принципами повышения эффективности 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	*Обучающийся знает:* основные методы управления информационной

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
информационной безопасностью	безопасностью
ПК-3.2.5. Умеет оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите	*Обучающийся умеет:* выявлять информационные активы автоматизированной системы, подлежащие защите, и оценивать их информационные риски

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)». (*вариативная часть)*

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		7
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	80 32 48	80 32 48
Самостоятельная работа (СРС) (всего)	28	28
Контроль	36	36
Форма контроля (промежуточной аттестации)	Э	Э
Общая трудоемкость: час / з.е.	144 / 4	144 / 4

Примечание: «Форма контроля» – экзамен (Э), зачет (З), зачет с оценкой (З), курсовой проект (КП), курсовая работа (КР)*

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Риски информационной безопасности	Лекция 1.1 Понятие и сущность риска	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лекция 1.2 Общая характеристика подходов к анализу и оцениванию риска	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лекция 1.3 Основные методы анализа риска (4 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лекция 1.4 Модели риска неготовности системы (4 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лекция 1.5 Основные методики и инструментальные средства оценки риска (8 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лабораторная работа №1 «Изучение стандартов в области управления рисками информационной безопасности» (8 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лабораторная работа №2 «Классификация и факторы рисков информационной безопасности типового предприятия» (8 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лабораторная работа №3 «Расчет рисков информационной безопасности для выбранного информационного ресурса» (8 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лабораторная работа № 4 «Объекты исследования рисков информационной безопасности» (12 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Литература: [1] – [9] Интернет-ресурсы [1] – [6]	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
2	Аудит информационной безопасности	Лекция 2.1 Нормативно-правовое обеспечение аудита информационной безопасности	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лекция 2.2 Процедура проведения аудита информационной безопасности	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лекция 2.3 Концепция аудита ИБ АСУ ТП (8 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Лабораторная работа №5 «Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer» (12 час)	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Литература: [1] – [9] Интернет-ресурсы [1] – [6]	ПК-2.3.3. ПК-3.1.1. ПК-3.2.5.

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Риски информационной безопасности	20		36	18	74

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
2	Аудит информационной безопасности	12		12	10	34
	Итого	32		48	28	108
					Контроль	36
					Всего (общая трудоемкость, час.)	144

6. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценочные материалы по дисциплине является неотъемлемой частью рабочей программы и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

7. 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, используя методические материалы дисциплины, а также учебно-методическое обеспечение, приведенное в разделе 8 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем успеваемости (см. оценочные материалы по дисциплине).
3. По итогам текущего контроля успеваемости по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. оценочные материалы по дисциплине).

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

8.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, 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, используемые для проведения учебных занятий и самостоятельной работы, соответствуют действующим санитарным и противопожарным нормам и правилам.

Для проведения лабораторных работ используется лаборатория кафедры «*Лаборатория защищенных автоматизированных систем»,* оборудованная следующими приборами/специальной техникой/установками используемыми в учебном процессе:

– Visual Studio C/C++

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;

– Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ».

8.3. 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.

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

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

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

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

2. Шапкин, А. С. Теория риска и моделирование рисковых ситуаций : учебник / А. С. Шапкин, В. А. Шапкин. — 6-е изд. — Москва : Дашков и К, 2017. — 880 с. — ISBN 978-5-394-02170-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/93446

3. Риск-модели информационной безопасности / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, А.А. Сидак – СПб.: Петербургский гос. ун-т путей сообщения, 2022. – 78 с.

4. Аудит и управление информационной безопасностью : учеб. пособие / А.А. Корниенко, С.В. Диасамидзе. – СПб.: Петербургский гос. ун-т путей сообщения, 2011. – 57 с.

Перечень нормативно-правовой документации, необходимой для освоения дисциплины

5. Стандарт Банка России СТО БР ИББС-1.1-2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности [Электронный ресурс]. – Разработан Банком России. – Введ. 2007-04-28. – Режим доступа: (http://www.cbr.ru).

6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. – Разработан Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем

технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИ ПТЗИ ФСТЭК России»). – Введ. 2008-02-01. – Режим доступа: (http://protect.gost.ru).

7. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации [Электронный ресурс]. – Разработан Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИ ПТЗИ ФСТЭК России»). – Введ. 2006-01-01. – Режим доступа: (http://protect.gost.ru).

8. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [Электронный ресурс]. – Режим доступа: (http://protect.gost.ru).

9. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. Обеспечение информационной безопасности Банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности [Электронный ресурс]. – Режим доступа: (http://www.cbr.ru).

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, проф. А.А. Корниенко
31.03.2025