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.2 «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»
для специальности
10.05.03 «*Информационная безопасность автоматизированных систем*»

по специализации
«*Безопасность автоматизированных систем на 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 «*Теоретические основы информационной безопасности автоматизированных систем» (Б1.В.02*) (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 угроз безопасности информации и моделей нарушителя в информационных системах;
- изучение основных принципов формирования политики безопасности в информационных системах;
- изучение базовых моделей разграничения доступа компьютерной системы
- изучение основных принципов антивирусной защиты автоматизированных систем.

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-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системах
- ПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ПК-1. Тестирование систем защиты информации автоматизированных систем	
ПК-1.1.3. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	*Обучающийся знает:* основные угрозы безопасности информации и модели нарушителя в информационных системах
ПК-1.1.4. Знает основные меры по защите информации в автоматизированных системах	*Обучающийся знает:* основные принципы реализации механизма идентификации/аутентификации и правил разграничения доступа
ПК-1.3.3. Имеет навыки	*Обучающийся владеет*

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
выявления основных угроз безопасности информации в автоматизированных системах	основными подходами к выявлению угроз безопасности информации в информационных системах
ПК-2. Разработка проектных решений по защите информации в автоматизированных системах	
ПК-2.1.5. Знает принципы формирования политики информационной безопасности в автоматизированных системах	*Обучающийся знает:* основные принципы формирования политики безопасности в информационных системах
ПК-2.2.2. Умеет определять типы субъектов доступа и объектов доступа, являющихся объектами защиты	*Обучающийся умеет:* представлять субъектно-объектную модель компьютерной системы
ПК-2.2.3. Умеет определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	*Обучающийся умеет:* проектировать наиболее подходящую модель разграничения доступа компьютерной системы на основе требований безопасности информации
ПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах	*Обучающийся владеет* основами разработки модели угроз безопасности информации информационной системы

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
		5
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)	60	60
Контроль	4	4
Форма контроля (промежуточной аттестации)	З, КП	З, КП
Общая трудоемкость: час / з.е.	144 / 4	144 / 4

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	Лекция 1.1. Основные понятия	ПК-1.1.3. ПК-1.1.4. ПК-1.3.3. ПК-2.1.5. ПК-2.2.2. ПК-2.2.3. ПК-2.3.1.
		Лекция 1.2 Основные виды формальных моделей безопасности	
		Лабораторная работа №1 «Требования к парольной системе защиты»» (6 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Выполнение курсового проекта. Подготовка к сдаче зачета). Литература: [1] – [8] Интернет-ресурсы [1] – [5]	
2	Основные виды моделей разграничения доступа	Лекция 2.1 Модель матрицы доступов Харрисона–Руззо–Ульмана	ПК-1.1.3. ПК-1.1.4. ПК-1.3.3. ПК-2.1.5. ПК-2.2.2. ПК-2.2.3. ПК-2.3.1.
		Лекция 2.2 Модель типизированной матрицы доступов	
		Лекция 2.3 Модель Белла–ЛаПадулы.	
		Лекция 2.4 Политика low-watermark.	
		Лекция 2.5 Базовая модель ролевого управления доступом.	
		Лекция 2.6 Администрирование ролевого управления доступом.	
		Лабораторная работа №2 «Моделирование механизма идентификации и аутентификации» (32 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Выполнение курсового проекта. Подготовка к сдаче зачета). Литература: [1] – [8] Интернет-ресурсы [1] – [5]	
3	Антивирусная защита автоматизированных систем	Лекция 3.1 Что такое компьютерный вирус.	ПК-1.1.3. ПК-1.1.4. ПК-1.3.3. ПК-2.1.5. ПК-2.2.2. ПК-2.2.3. ПК-2.3.1.
		Лекция 3.2 Общие сведения о методах борьбы с компьютерными вирусами.	
		Лекция 3.3 Классификация компьютерных вирусов.	
		Лекция 3.4 Общие принципы обнаружения вирусов.	
		Лекция 3.5 Статические методы детектирования вирусов.	
		Лекция 3.6 Эвристические методы детектирования вирусов.	
		Лекция 3.7 Концепция современного	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		антивирусного средства.	
		Лекция 3.8 Современные антивирусные средства	
		Лабораторная работа №3 «Изучение основ противодействия вредоносному ПО» (32 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Выполнение курсового проекта. Подготовка к сдаче зачета). Литература: [1] – [8] Интернет-ресурсы [1] – [5]	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	4		6	4	14
2	Основные виды моделей разграничения доступа	12		22	28	62
3	Антивирусная защита автоматизированных систем	16		20	28	64
	Итого	32		48	60	140
					Контроль	4
					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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: http://e.lanbook.com/book/63235.

2. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста.— М. : ДМК Пресс, 2013. — 656 с. — Режим доступа: http://e.lanbook.com/book/63192.

3. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 448 с.

4. Безопасность операционных систем: уч. пособие / С.В. Диасамидзе. – СПб: ФГБОУ ВО ПГУПС, 2017. – 76 с.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации№ от 27.07.2006 № 149-ФЗ;

6. ГОСТ Р 51188-98Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

7. Методические документы. Утверждены ФСТЭК России 14 июня 2012 г. Профили защиты средств антивирусной защиты

8. Моделирование механизма идентификации и аутентификации пользователей компьютерной системы: методические указания к выполнению лабораторных работ по дисциплине "Теоретические основы компьютерной безопасности" / СПб : ФГБОУ ВПО ПГУПС, 2014. - 24 с.

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