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.ДВ.1.2 «АНАЛИЗ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 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 «*Анализ безопасности программного обеспечения автоматизированных систем» (Б1.В.ДВ.1.2*) (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 инструментальных средств анализа автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности;
- овладение навыками тестирования программного и аппаратного обеспечения, в том числе систем защиты информации автоматизированных систем;
- овладение навыками разработки и использования технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты 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-1.3.1. Имеет навыки 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

ПК-1.3.4. Имеет навыки составления методик тестирования систем защиты информации автоматизированных систем

ПК-1.3.5. Имеет навыки подбора инструментальных средств тестирования систем защиты информации автоматизированных систем

ПК-1.3.6. Имеет навыки составления протоколов тестирования систем защиты информации автоматизированных систем

ПК-3.3.2. Имеет навыки анализа защищенности информационной инфраструктуры автоматизированной системы

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 автоматизированных систем

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ПК-1. Тестирование систем защиты информации автоматизированных систем	
ПК-1.2.2. Умеет анализировать основные узлы и устройства современных автоматизированных систем	*Обучающийся умеет:* проводить анализ архитектуры автоматизированной системы
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	*Обучающийся владеет* основными методами выявления уязвимостей информационной безопасности автоматизированной системы
ПК-1.3.2. Имеет навыки выявления уязвимости информационно-технологических ресурсов автоматизированных систем	*Обучающийся владеет* основными методами выявления уязвимостей информационной безопасности автоматизированной системы
ПК-1.3.4. Имеет навыки составления методик тестирования систем защиты информации автоматизированных систем	*Обучающийся владеет* принципами разработки методик испытаний программных и технических средств по требованиям безопасности информации
ПК-1.3.5. Имеет навыки подбора инструментальных средств тестирования систем защиты информации автоматизированных систем	*Обучающийся владеет* основными принципами применения инструментальных средств испытаний программных и технических средств по требованиям безопасности информации
ПК-1.3.6. Имеет навыки составления протоколов тестирования систем защиты информации автоматизированных систем	*Обучающийся владеет* принципами составления протоколов испытаний программных и технических средств по требованиям безопасности информации
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	*Обучающийся знает:* основные нормативные и методические документы в области защиты информации
ПК-3. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем	
ПК-3.1.2. Знает информационные воздействия и критерии оценки защищенности автоматизированных систем	*Обучающийся знает:* основные методы и критерии оценки защищенности автоматизированных

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
	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	*Обучающийся умеет:* применять основные методы выявления уязвимостей информационной безопасности автоматизированной системы
ПК-3.2.7.Умеет проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации	*Обучающийся умеет:* проводить тестирование и отладку программных и технических средств защиты информации
ПК-3.3.2. Имеет навыки анализа защищенности информационной инфраструктуры автоматизированной системы	*Обучающийся владеет* основными принципами анализа защищенности информационной инфраструктуры автоматизированной системы
ПК-4. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	
ПК-4.1.4. Знает принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения	*Обучающийся знает:* основы документирования процессов жизненного цикла программных и технических средств
ПК-4.1.5. Знает методы тестирования и отладки программного и аппаратного обеспечения	*Обучающийся знает:* основные методы тестирования и отладки программных и технических средств защиты информации
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	*Обучающийся умеет:* разрабатывать технические задания на программные или технические средства защиты информации
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 автоматизированных систем	*Обучающийся владеет* основами разработки технической документации на программные и технические средства защиты информации

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, дисциплины по выбору)*

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		А
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	96 32 64	96 32 64
Самостоятельная работа (СРС) (всего)	48	48
Контроль	36	36
Форма контроля (промежуточной аттестации)	Э	Э
Общая трудоемкость: час / з.е.	180 / 5	180 / 5

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	Подтверждение соответствия информационно-управляющих и автоматизированных систем	Лекция 1.1 Техническое регулирование и подтверждение соответствия	ПК-1.2.2. ПК-1.3.1. ПК-2.1.1. ПК-3.1.2. ПК-3.2.4. ПК-3.3.2. ПК-4.1.4. ПК-4.2.1. ПК-4.3.1.
		Лекция 1.2 Жизненный цикл программного обеспечения автоматизированных систем	
		Лекция 1.3 Показатели качества и защищенности программного обеспечения в ГОСТ 28195-89 и ГОСТ Р ИСО МЭК 9126-93	
		Лабораторная работа №1 «Разработка технического задания на средство защиты информации» (18 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [1] – [3] Интернет-ресурсы [1] – [5]	
2	Сертификация средств защиты информации по требованиям безопасности информации	Лекция 2.1 Система сертификации по требованиям безопасности информации	ПК-1.3.1. ПК-1.3.2. ПК-1.3.4. ПК-1.3.5. ПК-1.3.6. ПК-2.1.1. ПК-3.1.2. ПК-3.2.4. ПК-3.2.7. ПК-3.3.2. ПК-4.1.4. ПК-4.3.1.
		Лекция 2.2 Основные положения процесса сертификации по требованиям безопасности информации	
		Лекция 2.3 Основы сертификации средств защиты информации	
		Лекция 2.4 Сертификация средств вычислительной техники по требованиям защищенности от НСД к информации	
		Лекция 2.5 Сертификация межсетевых экранов по требованиям защищенности	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		от НСД к информации	
		Лекция 2.6 Сертификация программного обеспечения на отсутствие недекларированных возможностей (НДВ)	
		Лекция 2.7 Сертификация средств защиты информации в соответствии с методологией «Общих критериев»	
		Лабораторная работа №2 «Разработка программы и методики испытаний межсетевого экрана по требованиям безопасности информации» (18 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [3] Дополнительная литература: [1], [2] Нормативные документы: [1] – [6] Интернет-ресурсы [1] – [5]	
3	Методы и инструментальные средства анализа безопасности программного обеспечения	Лекция 3.1 Классификация уязвимостей и недекларированных возможностей программ	ПК-1.3.1. ПК-1.3.2. ПК-1.3.4. ПК-1.3.5. ПК-1.3.6. ПК-2.1.1. ПК-3.1.2. ПК-3.2.4. ПК-3.2.7. ПК-3.3.2. ПК-4.1.4. ПК-4.1.5. ПК-4.3.1.
		Лекция 3.2 Анализ и оценка безопасности программного обеспечения	
		Лекция 3.3 Методы контроля исходного состояния программного обеспечения	
		Лекция 3.4 Методы автоматизированного поиска уязвимостей программ	
		Лекция 3.5 Методы статического анализа программного кода	
		Лекция 3.6 Методы динамического анализа программ	
		Лабораторная работа №3 «Проведение испытаний на отсутствие недекларированных возможностей ПО» (28 час)	
		Самостоятельная работа (Повторение лекционного материала. Проработка вопросов самостоятельного обучения. Подготовка к лабораторным работам. Подготовка к сдаче экзамена). Основная литература: [3] Дополнительная литература: [1], [2] Нормативные документы: [1] – [6] Интернет-ресурсы [1] – [5]	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Подтверждение соответствия информационно-управляющих и автоматизированных систем	6		18	8	32
2	Сертификация средств защиты информации по требованиям безопасности информации	14		18	16	48
3	Методы и инструментальные средства анализа безопасности программного обеспечения	12		28	24	64
	Итого	32		64	48	144
					Контроль	36
					Всего (общая трудоемкость, час.)	180

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 верификации и оценки соответствия средств защиты информации»* оборудованная следующими приборами/специальной техникой/установками используемыми в учебном процессе:

– Программа фиксации и контроля исходного состояния программного комплекса "Трафарет 2.0"

– ФИКС (версия 2.0.2) Программа фиксации и контроля исходного состояния программного комплекса
– АИСТ-С Анализатор исходных текстов С и С++ программ
– Ревизор 2 XP Программа контроля полномочий доступа к информационным ресурсам

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: 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. Корниенко А.А., Диасамидзе С.В. Подтверждение соответствия и сертификация программного обеспечения по требованиям безопасности информации (учебное пособие). - СПб.: ПГУПС, 2009. – 55 с.

4. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. [Электронный ресурс] — Электрон.дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/book/5163

5. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ;

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

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

8. Указ Президента Российской Федерации «Вопросы Федеральной службы по техническому и экспортному контролю» от 16.08.2004 № 1085

9. Постановление Правительства Российской Федерации от 21.11.2011 № 957 «Об организации лицензирования отдельных видов деятельности»

10. Постановление Правительства Российской Федерации от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»

11. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

12. Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»

13. Положение о сертификации средств защиты информации по требованиям безопасности информации, введенное в действие приказом Председателя Гостехкомиссии России от 27.10.1995 № 199

14. Правила по проведению сертификации в Российской Федерации, утвержденные постановлением Госстандарта России от 10.05.2000 № 26

15. Порядок проведения сертификации продукции в Российской Федерации, утвержденный постановлением Госстандарта России от 21.09.1994 № 15

16. Положение от 27.10.1995 № 199 «О сертификации средств защиты информации по требованиям безопасности информации»

17. Положение по аттестации объектов информатизации по требованиям безопасности информации, утв. Гостехкомиссией РФ от 25.11.1994

18. ГОСТ Р ИСО/МЭК 17025-2006. Общие требования к компетентности испытательных и калибровочных лабораторий.

19. ГОСТ Р ИСО 9001-2008. Системы менеджмента качества. Требования.

20. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководство по их применению.

21. ГОСТ 28195-89. Оценка качества программных средств. Общие положения.

22. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. - М.: ИПК Издательство стандартов, 2006.

24. Методические документы. Утверждены ФСТЭК России 8 февраля 2018 г. Профили защиты операционных систем типа "А"

25. Методические документы. Утверждены ФСТЭК России 12 сентября 2016 г. Профили защиты межсетевых экранов

26. Методические документы. Утверждены ФСТЭК России 1 декабря 2014 г. Профили защиты средств контроля съемных машинных носителей информации

27. Методические документы. Утверждены ФСТЭК России 30 декабря 2013 г. Профили защиты средств доверенной загрузки

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

29. Методические документы. Утверждены ФСТЭК России 6 марта 2012 г. Профили защиты систем обнаружения вторжений

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