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.О.33 «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»*

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 «*Программно-аппаратные средства защиты информации» (Б1.О.33*) (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 формирование у обучающихся способности использовать программно-аппаратные средства защиты информации при решении задач профессиональной деятельности.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний о принципах функционирования программно-аппаратных средств для защиты информации в автоматизированных системах;
- формирование у обучающихся умений, связанных с разработкой и анализом программно-аппаратных средств защиты информации и их моделей;
- формирование у обучающихся навыков использования и исследования программно-аппаратных средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

## 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:

- использования и исследования программно-аппаратных средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач.

| **Индикаторы достижения компетенций** | **Результаты обучения по дисциплине (модулю)** |
|---|---|
| ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем | |
| ОПК-11.1.1. Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем | Обучающийся *знает*:<br>– основные принципы создания программно-аппаратных средств защиты информации;<br>– концепции построения диспетчера доступа;<br>– методы и средства ограничения доступа к компонентам вычислительных систем;<br>– методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; |

| Индикаторы достижения компетенций | Результаты обучения по дисциплине (модулю) |
|---|---|
| | – методы и средства хранения ключевой информации;<br>– способы встраивания средств защиты информации в программное обеспечение;<br>– основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. |
| ОПК-11.3.2. Имеет навыки применения программных и аппаратных компонентов, разрабатываемых различными фирмами-производителями, при построении систем защиты информации | Обучающийся *имеет навыки*:<br>– использовать на практике, основные, представленные на рынке, программно-аппаратные средства защиты информации;<br>– выполнять привязку программного обеспечения системы защиты информации к аппаратному окружению и физическим носителям;<br>– использовать техническую документацию для корректной и непротиворечивой настройки механизмов безопасности программно-аппаратных средств обеспечения информационной безопасности;<br>– использовать средства хранения ключевой информации и способы встраивания аппаратных компонентов средств защиты в программное обеспечение;<br>– оценивать эффективность и надежность функционирования программно-аппаратных средств обеспечения информационной безопасности;<br>– выявлять уязвимости защиты программно-аппаратных средств защиты информации и предотвращать их использование для взлома защиты;<br>– разрабатывать предложения по совершенствованию применения программно-аппаратных средств защиты информации на предприятии;<br>– администрирования программно-аппаратных средств защиты информации в автоматизированных и информационно-управляющих системах на транспорте;<br>– владения профессиональной терминологией в области программно-аппаратных средств защиты информации;<br>– корректного использования программно-аппаратных средств защиты информации. |

## 3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части блока 1 «Дисциплины (модули)».

## 4. Объем дисциплины и виды учебной работы

| Вид учебной работы | Всего часов | Модуль | |
|---|---|---|---|
| | | 7 | 8 |
| Контактная работа (по видам учебных занятий)<br>В том числе:<br>– лекции (Л)<br>– практические занятия (ПЗ)<br>– лабораторные работы (ЛР) | <br><br>64<br>-<br>96 | <br><br>32<br>-<br>48 | <br><br>32<br>-<br>48 |
| Самостоятельная работа (СРС) (всего) | 56 | 28 | 28 |
| Контроль | 72 | 36 | 36 |
| Форма контроля (промежуточной аттестации) | | Э | Э |
| Общая трудоемкость: час / з.е. | 288/8 | 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 |
|---|---|---|---|
| Модуль 1 (7 семестр) | | | |
| 1 | Архитектура систем защиты информации | Лекция 1. Введение. Требования к защите компьютерной информации | ОПК-11.1.1, ОПК-11.3.2 |
| | | Лекция 2. Анализ защищенности современных ОС (4 часа) | |
| | | Лекция 3. Подходы к проектированию системы защиты | |
| | | Лекция 4. Оценивание эффективности СЗИ при их проектировании | |
| | | Лекция 5. Особенности проектирования СЗИ. Этапы проектирования СЗИ (4 часа) | |
| | | Лекция 6. Системный подход к проектированию систем защиты информации | |
| | | Лекция 7. Архитектура СЗИ | |
| | | Лекция 8. Особенности архитектуры сетевой СЗИ. Состав и назначение функциональных блоков | |
| | | Лекция 9. Анализ эффективности ЦРА СЗИ (20 часов) | |
| | | Лабораторная работа № 1. Файловый сейф (12 часов) | |
| | | Лабораторная работа № 2. Персональный экран (12 часов) | |
| | | Лабораторная работа № 3. Система обнаружения вторжений (12 часов) | |

| № п/п | Наименование раздела дисциплины | Содержание раздела | Индикаторы достижения компетенций |
|---|---|---|---|
| | | Самостоятельная работа:<br>− изучение соответствующего раздела учебника [2];<br>− подготовка к лабораторным работам;<br>− изучение руководящих документов [3] и [4];<br>− подготовка к выполнению тестового задания по лекционному материалу 7 семестра[1]. | |
| 2 | Авторизация и управление доступом | Лекция 10. Авторизация и ее задачи (4 часа) | ОПК-11.1.1, ОПК-11.3.2 |
| | | Лекция 11. Добавочные механизмы парольной защиты (4 часа) | |
| | | Лабораторная работа № 4 Взлом парольной защиты (12 часов) | |
| | | Самостоятельная работа:<br>– изучение соответствующего раздела учебника [2];<br>– изучение руководящих документов [3], [4];<br>– подготовка к выполнению лабораторной работы;<br>– подготовка к выполнению тестового задания по лекционному материалу 7 семестра. | ОПК-11.1.1, ОПК-11.3.2 |
| Модуль 2 (8 семестр) | | | |
| 3 | Модели управления доступом | Лекция 12. Классификация субъектов и объектов доступа. Угрозы преодоления правил разграничения доступа к информации | ОПК-11.1.1, ОПК-11.3.2 |
| | | Лекция 13. Канонические модели управления доступом | |
| | | Лекция 14. Реализация моделей доступа | |
| | | Лекция 15. Общие положения по реализации управления доступом | |
| | | Лекция 16. Анализ возможностей корректной реализации моделей управления доступом встроенными в ОС механизмами защиты. | |
| | | Лекция 17. Субъект доступа «процесс» и его учет при разграничении доступа | |
| | | Лекция 18. Механизмы принудительного использования оригинальных приложений. | |
| | | Лекция 19. Локализация прав доступа стандартных приложений к ресурсам (16 часов) | |
| | | Лабораторная работа №5. Исследование типовой клиентской части системы защиты информации для отдельной рабочей станции в составе локальной вычислительной сети (12 часов) | |

[1] Тестовые задания по лекционному материалу 7 и 8 семестров размещены в ЭИОС в соответствующем разделе дисциплины «Программно-аппаратные средства защиты информации и выполняются по указанию преподавателя.

| № п/п | Наименование раздела дисциплины | Содержание раздела | Индикаторы достижения компетенций |
|---|---|---|---|
| | | Лабораторная работа №6. Исследование сетевой системы защиты информации, построенной по клиент-серверной технологии (12 часов). | |
| | | Самостоятельная работа:<br>– изучение соответствующего раздела учебника [2];<br>– изучение руководящих документов [3], [4];<br>– подготовка к выполнению лабораторной работы;<br>– подготовка к выполнению тестового задания по лекционному материалу 8 семестра. | ОПК-11.1.1, ОПК-11.3.2 |
| 4 | Реализация механизмов защиты | Лекция 20. Диспетчер доступа. Механизм замкнутой программной среды. | ОПК-11.1.1, ОПК-11.3.2 |
| | | Лекция 21. Формальная модель диспетчера доступа | |
| | | Лекция 22. Модель рабочей станции без системы защиты | |
| | | Лекция 23. Модель рабочей станции с системой защиты | |
| | | Лекция 24. Централизация администрирования системой защиты информации. Механизм обеспечения целостности. | |
| | | Лекция 25. Использование аппаратных средств защиты | |
| | | Лекция 26. Противодействие переводу программного обеспечения системы защиты информации в пассивное состояние в процессе функционирования системы. | |
| | | Лекция 27. Реализация механизмов контроля вскрытия аппаратуры. Заключение (16 часов). | |
| | | Лабораторная работа №7. Построение модели типовой защищённой локальной вычислительной сети и исследование её характеристик (12 часов). | |
| | | Лабораторная работа №8. Исследование способов организации скрытого электронного документооборота и методов его обнаружения (12 часов). | |
| | | Самостоятельная работа:<br>– изучение соответствующего раздела учебника [2];<br>– изучение руководящих документов [3], [4];<br>– подготовка к выполнению лабораторной работы;<br>– подготовка к выполнению тестового задания по лекционному материалу 8 семестра. | ОПК-11.1.1, ОПК-11.3.2 |

5.2. Разделы дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Л | ПЗ | ЛР | СРС | Всего |
|---|---|---|---|---|---|---|
| Модуль 1 (7 семестр) | | | | | | |
| 1 | Архитектура систем защиты информации | 24 | 0 | 36 | 20 | 80 |
| 2 | Авторизация и управление доступом | 8 | 0 | 12 | 8 | 28 |
| | **Итого** | 32 | 0 | 48 | 28 | 108 |
| | | | | | **Контроль** | 36 |
| | | | | | **Всего** (общая трудоемкость, час.) | 144 |

| № п/п | Наименование раздела дисциплины | Л | ПЗ | ЛР | СРС | Всего |
|---|---|---|---|---|---|---|
| Модуль 2 (8 семестр) | | | | | | |
| 3 | Модели управления доступом | 16 | 0 | 24 | 14 | 54 |
| 4 | Реализация механизмов защиты | 16 | 0 | 24 | 14 | 54 |
| | **Итого** | 32 | 0 | 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 являются 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 программно-аппаратных средств обеспечения информационной безопасности, оборудованная компьютерной техникой с установленными программными средствами системы защиты информации, перечисленными в п. 8.2.

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;

– 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/);

– криптографическая библиотека OpenSSL (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://www.openssl.org/).

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" – 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.

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

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

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


1. А.А. Корниенко, С. Е. Ададуров, А.П. Глухов и др. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / 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. А.А. Корниенко, С. Е. Ададуров, А.П. Глухов и др. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / 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. РД Гостехкомиссии: Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. – М.:1992.
4. РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992.
5. Технические средства и методы защиты информации : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - [4-е изд., испр. и доп.]. - Москва : Горячая линия - Телеком, 2012. - 615 с.
6. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. - 7-е изд. - Москва : Горячая линия - Телеком, 2012. - 442 с.


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

– Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://my.pgups.ru — Режим доступа: для авторизованных пользователей;

– Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://sdo.pgups.ru — Режим доступа: для авторизованных пользователей;

– Электронный фонд правовой и нормативно-технической документации – URL: http://docs.cntd.ru/ — Режим доступа: свободный.

Разработчик рабочей программы, *доцент* *М.Л. Глухарев*
18.03.2025 г.