

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.38 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

для специальности

*10.05.03 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ»*

по специализации

«Безопасность автоматизированных систем на железнодорожном транспорте»

Форма обучения – очная

Санкт-Петербург
2026

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и утверждена на заседании кафедры «Информатика и информационная безопасность»

Протокол № 6 от 28 января 2026 г.

И.о. заведующего кафедрой
«Информатика и информационная безопасность»
28 января 2026 г.

К.З. Билятдинов

СОГЛАСОВАНО

Руководитель ОПОП
28 января 2026 г.

М.Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа дисциплины «Управление информационной безопасностью» (Б1.О.38) (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 администрировать и контролировать функционирование средств и систем защиты информации автоматизированных систем, проводить инструментальный мониторинг защищенности автоматизированных систем, применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний о методологии управления информационной безопасностью, основанной на нормативных и методических документах, об основных методах администрирования и контроля функционирования средств и систем защиты информации при проведении мониторинга и аудита защищенности автоматизированных систем;
- формирование у обучающихся умений администрировать средства и системы защиты информации автоматизированных систем;
- формирование у обучающихся базовых навыков контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем, проведения инструментального мониторинга и аудита защищенности 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:

- контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем;
- проведения инструментального мониторинга и аудита защищенности автоматизированных систем.

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	
ОПК-5.1.2. Знает методологию управления информационной	Обучающийся <i>знает</i> : – подходы к обеспечению и управлению информационной безопасностью;

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
безопасностью, основанную на нормативных и методических документах	– процессную модель управления информационной безопасностью; – автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте; – способы управления рисками информационной безопасности; – модель управления инцидентами информационной безопасности; – процесс управления инцидентами информационной безопасности
ОПК-15. Способен проводить администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	
ОПК-15.1.1. Знает основные методы администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем	Обучающийся <i>знает</i>: – методы и средства администрирования в MS Windows и Linux; – инструменты управления доступностью к ресурсам; – способы управление доступом к информации автоматизированных систем; – правление корпоративной сетью; – особенности применения искусственного интеллекта и системы поддержки и принятия решений в системах управления информационной безопасностью
ОПК-15.1.2. Знает основные методы инструментального мониторинга и аудита защищенности автоматизированных систем	Обучающийся <i>знает</i>: – способы проведения активного аудита информационной безопасности; – приёмы расследования инцидентов и разработка превентивных мер; – системы предотвращения вторжений; – системы предотвращения утечек
ОПК-15.2.1. Умеет администрировать средства и системы защиты информации автоматизированных систем	Обучающийся <i>умеет</i> администрировать: – средства активного аудита; – системы обнаружения вторжений; – системы предотвращения утечек
ОПК-15.3.1. Имеет базовые навыки контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем	Обучающийся <i>имеет навыки</i>: – применения средств удалённого управления информационной безопасностью; – управления пользователями; – контроля паттернов инцидентов информационной безопасности
ОПК-15.3.2. Имеет базовые навыки проведения инструментального мониторинга и аудита защищенности автоматизированных систем	Обучающийся <i>имеет навыки</i>: – администрировать средства активного аудита в MS Windows и Linux; – управления адресацией и именами автоматизированных систем в ходе применения средств мониторинга и аудита защищённости

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
Контактная работа (по видам учебных занятий) В том числе:	
– лекции (Л)	32
– практические занятия (ПЗ)	-
– лабораторные работы (ЛР)	64
Самостоятельная работа (СРС) (всего)	48
Контроль	36
Форма контроля (промежуточной аттестации)	
Общая трудоемкость: час / з.е.	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
Семестр А			
1	Методология управления информационной безопасностью	Лекция 1. Подходы к обеспечению и управлению информационной безопасностью	ОПК-5.1.2, ОПК-15.1.1, ОПК-15.1.2
		Лекция 2. Процессная модель управления информационной безопасностью	
		Лекция 3. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте	
		Лекция 4. Управление рисками информационной безопасности	
		Лекция 5. Модель управления инцидентами информационной безопасности	
		Лекция 6. Процесс управления инцидентами информационной безопасности	
		Лабораторная работа 1. Описание бизнес-процессов транспортно-логистических систем с точки зрения информационной безопасности (4 часа)	ОПК-5.1.2, ОПК-15.1.1, ОПК-15.1.2, ОПК-15.2.1, ОПК-15.3.1, ОПК-15.3.2
		Лабораторная работа 2. Формирование модели угроз транспортно-логистических систем (4 часа)	
		Лабораторная работа 3. Работа с неструктурированными данными в информационной безопасности (4 часа)	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лабораторная работа 4. Построение модели нарушителя информационной безопасности транспортно-логистической системы (4 часа)	
		Лабораторная работа 5. Разработка политики безопасности (8 часов)	
		Самостоятельная работа: – изучение части 1 учебника [1]; – изучение нормативных документов [11-25]; – подготовка к лабораторным работам [2-7].	ОПК-5.1.2, ОПК-15.1.1, ОПК-15.1.2, ОПК-15.2.1, ОПК-15.3.1, ОПК-15.3.2

2	Технические аспекты управления информационной безопасностью	Лекция 7. Средства аудита информационной безопасности Windows	ОПК-5.1.2, ОПК-15.1.1, ОПК-15.1.2, ОПК-15.2.1, ОПК-15.3.1, ОПК-15.3.2
		Лекция 8. Средства аудита информационной безопасности Linux/Unix	
		Лекция 9. Активный аудит информационной безопасности	
		Лекция 10. Расследование инцидентов и разработка превентивных мер	
		Лекция 11. Системы предотвращения вторжений	
		Лекция 12. Системы предотвращения утечек	
		Лекция 13. Управление доступностью к ресурсам	
		Лекция 14. Управление доступом	
		Лекция 15. Управление корпоративной сетью	
		Лекция 16. Искусственный интеллект и системы поддержки и принятия решений в СУИБ	
		Лабораторная работа 6. Применение средств активного аудита в Windows (4 часа)	
		Лабораторная работа 7. Применение средств активного аудита в Linux (4 часа)	
		Лабораторная работа 8. Проведение тестов на проникновение (4 часа)	
		Лабораторная работа 9. Паттерны инцидентов информационной безопасности (4 часа)	
		Лабораторная работа 10. Настройка IDS (4 часа)	
		Лабораторная работа 11. Настройка DLP-системы (4 часа)	
		Лабораторная работа 12. Управление доступностью к ресурсам (4 часа)	
		Лабораторная работа 13. Управление пользователями (4 часа)	
		Лабораторная работа 14. Управление адресацией и именами автоматизированных систем (4 часа)	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Лабораторная работа 10. Применение средств удалённого администрирования ssh, RDP (4 часа)	
		Самостоятельная работа: – изучение 2 части 1 учебника [2]; – подготовка к выполнению лабораторных работ [8-10].	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
Семестр А						
1	Методология управления информационной безопасностью	12	0	24	18	24
2	Технические аспекты управления информационной безопасностью	20	0	40	30	90
	Итого	32	0	64	28	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, 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 обеспечения информационной безопасности и виртуализации, 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:

Перечень лицензионных программ представлен на внутреннем портале ФГБОУ ВО ПГУПС по адресу <http://eaisu.pgups.edu.mps/info/prog/>

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. 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. Аудит и управление информационной безопасностью (учебное пособие). – СПб.: ПГУПС, 2011. – 83 с.

4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. – М.: Горячая линия–Телеком, 2014. – 244 с.

5. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. – М.: Горячая линия–Телеком, 2014. – 130 с.

6. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие – М. : Горячая линия - Телеком, 2012. - 168 с.

7. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие - М.: Горячая линия - Телеком, 2012. - 214с.

8. П.Ю. Богданов, В.В. Грызунов, Е.П. Истомин, Т.М. Татарникова, Н.В. Яготинцева. Методы защиты информации. Учебное пособие. - СПб.: ООО «Андреевский издательский дом», 2019 - 74 с

9. В.Г. Бурлов, В.В. Грызунов. IT-инструменты для обработки, представления и передачи данных в исследовательской работе (учебное пособие).- СПб.: ООО «Андреевский издательский дом», 2018.- 96с.

10. В.В. Грызунов, Н.В. Яготинцева. Защита операционных систем (учебное пособие).- СПб.: ООО «Андреевский издательский дом», 2018.- 172с.

11. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

12. Федеральные законы:

- «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006;

- «О коммерческой тайне» № 119-ФЗ от 29.07.2004;

- «О персональных данных» № 152-ФЗ от 27.07.2006.

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

14. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

15. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3.

16. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

17. ГОСТ ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

18. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

19. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

20. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.- М.: Стандартинформ, 2012. -12 с.
21. СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения» // ОАО «РЖД», 2009.
22. Основные положения защиты информационной инфраструктуры ОАО «РЖД» // ОАО «РЖД», 2013.
23. Политика информационной безопасности ОАО «РЖД» // ОАО «РЖД», 2013.
24. Положение по оценке рисков информационной безопасности ОАО «РЖД» // ОАО «РЖД», 2015.
25. Положение по управлению инцидентами информационной безопасности в ОАО «РЖД» // ОАО «РЖД», 2014.

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 авториз. пользователей;
- Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: <https://sdo.pgups.ru> — Режим доступа: для авториз. пользователей;
- Электронный фонд правовой и нормативно-технической документации – URL: <http://docs.cntd.ru/> — Режим доступа: свободный.

Разработчик рабочей программы, *профессор*
23 01 2026 г.

В.В. Грызунов