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.37 «РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

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 *«Разработка и эксплуатация автоматизированных систем в защищенном исполнении» (Б1.О.37*) (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 методическое и правовое обеспечение процессов разработки и эксплуатации защищенных автоматизированных систем при решении задач профессиональной деятельности.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающихся знаний в области:
  - основных нормативных документов, государственных и международных стандартов в области разработки автоматизированных систем в защищенном исполнении (АС ЗИ);
  - порядок и содержание стадий и этапов создания АС ЗИ;
  - основные нормативные документы и стандарты в области эксплуатации АС ЗИ;
- формирование у обучающихся умений:
  - формировать требования к подсистемам информационной безопасности АС ЗИ;
  - осуществлять и обосновывать выбор элементной базы и средств защиты для АС ЗИ;
  - оценивать показатели риска АС ЗИ на этапах проектирования, испытаний и эксплуатации;
  - контролировать эффективность проектирования, разработки, внедрения и эксплуатации АС ЗИ;
- формирование у обучающихся навыков владения:
  - методами проектирования систем, удовлетворяющих заданным требованиям надежности и информационной безопасности;
  - методиками оценки показателей качества и эффективности АС ЗИ;
  - навыками участия в экспертизе состояния защищенности информации на объекте защиты.

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 владения методами поиска и анализа нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации и способами

применения действующей нормативной базы в области защиты информации ограниченного доступа в автоматизированных системах.

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*: − состав и содержание Российских законов, регламентирующих требования к подсистемам информационной безопасности АС ЗИ; − требования к выбору и сертификации элементной базы и средств защиты для АС ЗИ.
ОПК-11.2.1. Умеет разрабатывать компоненты защиты информации автоматизированных систем	Обучающийся *умеет*: – применять на практике методы и способы разработки компонент защиты информации автоматизированных систем; – контролировать эффективность проектирования, разработки, внедрения и эксплуатации АС ЗИ.
ОПК-11.3.1. Имеет навыки применения инструментальных средств поддержки всех этапов разработки компонентов систем защиты информации автоматизированных систем	Обучающийся имеет навыки: – проектирования систем, удовлетворяющих заданным требованиям надежности и информационной безопасности; – инструментального мониторинга защищенности информации в автоматизированной системе и выявлять каналы утечки информации
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей	
ОПК-13.1.1. Знает основы диагностики и тестирования систем защиты информации автоматизированных систем	Обучающийся *знает*: − основы диагностики и тестирования систем защиты информации автоматизированных систем.
ОПК-13.1.2. Знает базовые методы анализа уязвимостей систем защиты информации и моделирования угроз информационной безопасности	Обучающийся *знает*: − базовые модели уязвимостей автоматизированных систем. − базовые модели нарушителей. − базовые модели угроз.
ОПК-13.2.1. Умеет проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем	Обучающийся *умеет*: − оценивать показатели риска автоматизированных систем в защищенном исполнении на этапах проектирования, испытаний и эксплуатации; − создавать и исследовать модели автоматизированных систем;
ОПК-13.3.1. Имеет базовые навыки проведения	Обучающийся *имеет навыки*: − участия в экспертизе состояния защищенности

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
диагностики и тестирования систем защиты информации автоматизированных систем	информации на объекте защиты.
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированной системы с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	
ОПК-14.2.1. Умеет разрабатывать, внедрять в эксплуатацию, оценивать качество автоматизированных систем	Обучающийся *умеет*: – проводить анализ защищенности автоматизированных систем; – проводить анализ статистических данных об эксплуатации автоматизированных систем.
ОПК-14.3.1. Владеет базовыми методами проектирования, разработки, внедрения в эксплуатацию автоматизированных систем в защищенном исполнении	Обучающийся *имеет навыки*: – проектирования систем, удовлетворяющих заданным требованиям надежности и информационной безопасности; – обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций

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) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	144 64 - 80	64 32 - 32	80 32 - 48
Самостоятельная работа (СРС) (всего)	68	40	28
Контроль	40	4	36
Форма контроля (промежуточной аттестации)		З	Э
Общая трудоемкость: час / з.е.	252/7	108/3	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	Введение в дисциплину	Лекция 1. Предмет и задачи дисциплины. Научные основы дисциплины в системе подготовки специалистов в области АСЗИ. Основные понятия и определения, используемые в рамках дисциплины. Модели жизненного цикла безопасности АСЗИ.	ОПК-11.1.1, ОПК-11.2.1
		Самостоятельная работа: – изучение раздела 1 учебного пособия [5]; – ознакомление с основными положениями профстандарта [10], подготовка к выполнению тестового задания по лекционному материалу 8 семестра.	
2	Разработка и проектирование систем промышленной автоматики и контроля	Лекция 2. Система стандартов в области разработки автоматизированных систем (АС). Методология проектирования АС. Методология построения комплексных систем защиты информации (КСЗИ). Техническая документация АС.	ОПК-11.1.1, ОПК-11.2.1 ОПК-11.3.1
		Лекция 3. Основные принципы, условия, подходы и требования к системному и функциональному анализу АС. Методы и особенности функционального анализа АС.	
		Лекция 4. Содержание работ на этапах создания АС. Особенности этапа «Обследование и обоснование необходимости создания АС». Фаза «Анализ» жизненного цикла безопасности ПАЗ.	
		Лекция 5. Особенности стадии «Формирование требований пользователя к АС». Обоснование необходимости защиты информации в АС. Разработка спецификации требований к ПАЗ.	
		Лабораторная работа №1. Структура стандартов серии “Информационная технология».	
		Лабораторная работа №2. Методы функционального анализа АС. Методология IDEF0. Шаблон СТБ.	
		Самостоятельная работа: – изучение разделов 1-3 стандартов [18, 23, 27];	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		– углубленное изучение раздела 2.2 [6] – ознакомление с основными положениями раздела 2.2 [6], подготовка к выполнению тестового задания по лекционному материалу 8 семестра.	
3	Особенности разработки и проектирования АСЗИ	Лекция 6. Нормативные правовые акты, международные и национальные стандарты по области обеспечения защиты информации в автоматизированных системах.	ОПК-11.2.1, ОПК-11.3.1 ОПК-11.3.2
		Лекция 7. Основные информационные технологии, используемые в автоматизированных системах. Модели угроз безопасности информации в АС. Классификация мер обеспечения информационной безопасности.	
		Лекция 8. Модели жизненного цикла безопасности. Раздел «Информационная безопасность» ТЗ на разработку АС	
		Лекция 9. Формирование разделов технического задания на создание систем АСЗИ. Подсистемы комплексной системы защиты информации (КСЗИ).	
		Лекция 10. Программно-аппаратные средства обеспечения защиты информации в АС. Сертификация средств защиты информации в АС. Разработка архитектуры СЗИ АС.	
		Лабораторная работа №3. Исследование моделей автоматизированных систем и подсистем защиты информации АС. Основные меры по защите информации в АС	
		Лабораторная работа №4 . Формирование разделов технического задания на создание систем АСЗИ. Определение возможностей внешних и внутренних нарушителей.	
		Самостоятельная работа: – изучение разделов 2-5 [4] и п.15 [8]; – ознакомление с основными положениями раздела 4 и подраздела 1.3 [6], – ознакомление с основными положениями нормативного документа [13].	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		подготовка к выполнению тестового задания по лекционному материалу 8 семестра.	
4	Методы риск-ориентированного подхода к разработке систем промышленной автоматизации и контроля	Лекция 11. Методы анализа риска аварий промышленных предприятий. Понятие матрица риска.	ОПК-13.1.1, ОПК-13.1.2 ОПК-13.2.1
		Лекция 12. Распределение функций безопасности по независимым слоям защиты для решения задач функциональной безопасности.	
		Лекция 13. Определение структурно-функциональных характеристик АС в соответствии с требованиями нормативных документов в области функциональной и информационной безопасности.	
		Лекция 14. Методы анализа информационных рисков. Система менеджмента информационной безопасности. Реестр рисков.	
		Лекция 15. Классификация уязвимостей АС. Методика анализа уязвимостей.	
		Лекция 16. Анализ и оценка угроз информационной безопасности.	
		Лабораторная работа №5. Процедуры анализа опасностей и риска в области функциональной безопасности АСУТП	
		Лабораторная работа №6. Методика оценки показателей функциональной безопасности ПАЗ	
		Лабораторная работа №7. Методика разработки документов системы менеджмента функциональной безопасности	
		Лабораторная работа №8. Методика разработки документов системы менеджмента функциональной безопасности	
		Самостоятельная работа: – изучение основных положений Методик [16,17]; – ознакомление с основными положениями нормативных документов [11-15],	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		– изучение 1 и 2 разделов частей 1, 2 и 3 [35], – изучение основных положений стандарта [33], – изучение основных положений Приложения А стандарта [37] подготовка к выполнению тестового задания по лекционному материалу 8 семестра.	
5	Организация и функционирование системы эксплуатации АС	Лекция 17 Основные определения и понятия системы эксплуатации АС и СЗИ. Порядок установки и ввода в эксплуатацию АС.	ОПК-13.3.1, ОПК-14.2.1 ОПК-14.3.1
		Лекция 18. Концепция УРРАН. Задачи и структура информационных технологий комплексного управления эксплуатацией АС.	
		Лабораторная работа №9. Методы анализа статистических данных об эксплуатации АС.	
		Самостоятельная работа: – Содержание и основные положения учебного пособия [5]; подготовка к выполнению тестового задания по лекционному материалу 9 семестра.	
6	Организация и функционирование системы технической эксплуатации АС	Лекция 19. Организация функционирования системы технической эксплуатации АС. Приемо-сдаточные испытания компонент и подсистем.	ОПК-13.3.1, ОПК-14.2.1 ОПК-14.3.1
		Лекция 20. Подсистема технического обслуживания и ремонта. Общие понятия и терминология. Техническое обслуживание, ориентированное на безопасность.	
		Лабораторная работа №10. Основные эксплуатационные документы АСЗИ.	
		Самостоятельная работа: – Изучение раздела 9 [1]; – Углубление знаний стандартов по эксплуатации [42,43]. подготовка к выполнению тестового задания по лекционному материалу 9 семестра.	
7	Особенности организации и функционирование системы эксплуатации	Лекция 21. Объекты защиты и категории защищаемой информации в АС.	ОПК-13.3.1, ОПК-14.2.1 ОПК-14.3.1
		Лекция 22. Источники угроз и классификация угроз в АС.	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
	АСЗИ. Модели уязвимостей и угроз	Лекция 23. Способы реализации угроз безопасности информации. Рискобразующие факторы (уязвимости).	
		Лекция 24. Методика анализа актуальных угроз и оценка рисков информационной безопасности	
		Лабораторная работа №11. Определение актуальных угроз и оценка рисков информационной безопасности. Меры защиты информации при эксплуатации АС.	
		Самостоятельная работа: – Углубление знаний методик оценки и моделирования угроз ИБ [16,17]. подготовка к выполнению тестового задания по лекционному материалу 9 семестра.	
8	Особенности организации и функционирование системы технической эксплуатации АСЗИ. Модели уязвимостей и угроз. Модели нарушителей.	Лекция 25. Содержание и порядок деятельности персонала по эксплуатации АСЗИ. Контроль результатов деятельности действий персонала в области безопасности информации в АС	ОПК-13.1.2, ОПК-13.3.1, ОПК-14.2.1 ОПК-14.3.1
		Лекция 26. Содержание и правила ведения эксплуатационной документации АСЗИ.	
		Лекция 27. Разработка организационно-распорядительных документов по защите информации в АС. Модели нарушителя информационной безопасности АС.	
		Лекция 28. Правила и процедуры защиты информации при выводе АС из эксплуатации. Правила и процедуры реагирования на инциденты.	
		Лабораторная работа 12. Контроль качества комплектующих изделий системы защиты информации АС.	
		Лабораторная работа 13. Содержание и порядок проведения приемочных испытаний системы зашиты информации АС.	
		Лабораторная работа 14. Сценарное моделирование основных угроз безопасности АС и модели нарушителя	
		Лабораторная работа 15. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации.	
		Самостоятельная работа: – Углубление знаний методик оценки и моделирования угроз ИБ [16,17].	

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		подготовка к выполнению тестового задания по лекционному материалу 9 семестра.	
9	Методы анализа актуальных угроз и оценка рисков функциональной и информационной безопасности автоматизированных систем	Лекция 29. Концепция жизненного цикла безопасности систем промышленной автоматики и контроля (IACS). Этапы анализа риска и оценки уровня безопасности.	ОПК-13.1.2, ОПК-13.3.1, ОПК-14.2.1 ОПК-14.3.1
		Лекция 30. Методы анализа риска в задачах функциональной и информационной безопасности.	
		Лекция 31. Разработка и реализация системы менеджмента функциональной и информационной безопасности	
		Лекция 32. Заключительная лекция. Особенности и перспективы развития СХИ в АСУТП на опасных производственных объектах и объектах КИИ.	
		Лабораторная работа 16. Разработка методики проведения процедуры анализа опасностей и риска автоматизированных систем управления и защиты	
		Лабораторная работа 17. Методики сценарного моделирования обеспечения функциональной и информационной сложных АС.	
		Самостоятельная работа: – Углубление знаний методик оценки и моделирования угроз ИБ [16,17]. подготовка к выполнению тестового задания по лекционному материалу 9 семестра.	

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
Модуль 1 (7 семестр)						
1	Введение в дисциплину	2	-	-	2	4
2	Разработка и проектирование систем промышленной автоматики и контроля	8	-	8	8	24
3	Особенности разработки и проектирования АСЗИ	10	-	8	12	30
4	Методы анализа актуальных угроз и оценка рисков функциональной и	12	-	16	18	46

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
	информационной безопасности автоматизированных систем					
	Итого	32	0	32	40	104
					Контроль	4
					Всего (общая трудоемкость, час.)	108
Модуль 2 (8 семестр)						
5	Организация и функционирование системы эксплуатации автоматизированных систем	4	-	4	4	12
6	Организация и функционирование системы технической эксплуатации автоматизированных систем	4	-	4	4	12
7	Особенности организации и функционирование системы эксплуатации АСЗИ. Модели уязвимостей и угроз	8	-	8	6	22
8	Особенности организации и функционирование системы технической эксплуатации АСЗИ. Модели уязвимостей и угроз. Модели нарушителей.	8	-	16	6	30
9	Методы анализа актуальных угроз и оценка рисков функциональной и информационной безопасности автоматизированных систем	8	-	16	8	32
	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.

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

1. Скляр В.В. Обеспечение безопасности АСУТП в соответствии с современными стандартами, - М.: Инфра-Инженерия, 2018.-384с.
2. Струков А.В. Логико-вероятностное моделирование надежности и безопасности в задачах разработки и эксплуатации защищенных автоматизированных систем. Учебное пособие. - ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2020. – 73с.
3. Федоров Ю.Н. Основы построения АСУТП взрывоопасных производств. Том 1: Методология. М.: СИНТЕГ, 2006, 720с.
4. Федоров Ю.Н. Основы построения АСУТП взрывоопасных производств. Том 2: Проектирование. М.: СИНТЕГ, 2006, 632с.
5. Корниенко А.А. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте. - ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2016. -45с.
6. Перепечёнов А.М. Основы проектирования защищенных информационных систем/ А.М. Перепечёнов. - ФГБОУ ВО ПГУПС. – Санкт-Петербург. 2013. -59с.
7. Заляжных В.А., Гирик А.В. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммутационных систем.- СПб. Университет ИТМО, 2014-136с.
8. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации. - СПб. Университет ИТМО, 2011-112с.
9. Конспект лекций. Электронная информационно-образовательная среда. Раздел дисциплины Разработка и эксплуатация защищенных автоматизированных систем. [Электронный ресурс]. – URL: https://sdo.pgups.ru/course/view.php?id=2082 — Режим доступа: для авторизованных пользователей.
10. Профессиональный стандарт "Специалист по защите информации в автоматизированных системах". Утвержден постановлением Правительства Российской Федерации от 22 января 2013 года N 23/
11. Федеральный закон Российской Федерации от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. Приказ ФСТЭК №17 от 11.02.2013г. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
13. Приказ ФСТЭК №675 от 11.02.2014г. «Методический документ. Меры защиты информации в государственных информационных системах».
14. Приказ ФСТЭК №31 от 14.03.2013г. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды».
15. Приказ ФСТЭК №235 от 21.12.2017г. "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и требованию их функционированию".

16. Приказ ФСТЭК №239 от 25.12.2017г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
17. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК РОССИИ 5 февраля 2021г.
18. Методический документ. Методика моделирования угроз безопасности информации. Проект. ФСТЭК РОССИИ 2020г.
19. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
20. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
21. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
22. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Техническое задание на создание автоматизированной системы.
23. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем.
24. ГОСТ 24.104-85. Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования.
25. ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения
26. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
27. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.
28. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
29. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
30. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
31. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
32. ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.
33. ГОСТ Р ИСО/МЭК 27000-2021. Методы и средства обеспечения безопасности. Общий обзор и терминология.
34. ГОСТ Р ИСО/МЭК 27005-2010. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
35. ГОСТ Р 58833-202. Защита информации. Идентификация и аутентификация. Общие положения.

36. ГОСТ Р МЭК 61508-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Части 1-7.
37. ГОСТ Р МЭК 61511-2018. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Части 1-3.
38. ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009). Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.
39. ГОСТ Р МЭК 62443-2-1-2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики.
40. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Часть 3-3. Требования к системной безопасности и уровни безопасности.
41. ГОСТ 25866-83 Эксплуатация техника. Термины и определения.
42. ГОСТ 18322-2016. Система технического обслуживания и ремонта техники. Термины и определения.
43. ГОСТ Р 27.601-2011 Надежность в технике. Управление надежностью. Техническое обслуживание и его обеспечение.
44. ГОСТ Р 27.606-2013 Надежность в технике. Управление надежностью. Техническое обслуживание, ориентированное на безотказность.

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

- ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru

– 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*
23.03.2025 г. *А. В. Струков*