Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2026
Владелец: к.т.н. Рева И. Л.
Срок действия: не ограничен
Адрес хранения электронного документа:
https://www.nstu.ru/university/info/sveden/education

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Разработка и эксплуатация защищённых автоматизированных систем

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Безопасность значимых объектов критической информационной инфраструктуры

Курс: 5, семестр : 9

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**9**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	76
4	Лекции, час.	36
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	0
8	из них практической подготовки, час.	18
9	Аттестация, час.	2
10	Консультации, час.	20
11	Самостоятельная работа, час.	104
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	
13	Вид аттестации	Э

Новосибирск 2026

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1457 от 26.11.2020 г. , дата утверждения: 17.02.2021 г.

Место дисциплины в структуре учебного плана: Блок 1, формируемая участниками образовательных отношений

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, 31.08.2026

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 8 от 31.08.2026

Заведующий кафедрой:

доцент, к.т.н. Иванов А. В.

Ответственный за образовательную программу:

заведующий кафедрой Иванов А. В.

1. Внешние требования

Таблица 1.1

Группа	Компетенции
	Индикаторы достижения компетенций
Профессиональные компетенции	ПК-2.В/ОУ Способен организовывать работы по защите информации на объектах информатизации
	ПК-2.В/ОУ. 2 Умеет осуществлять планирование и организацию работ по защите информации с учётом требований по информационной безопасности
Профессиональные компетенции	ПК-3.В/КА Способен осуществлять контрольно-аналитическую дея-тельность и оценивать уровень безопасности систем защиты информации и их компонентов
	ПК-3.В/КА. 2 Умеет оценивать уровень безопасности систем защиты информации и их компонентов
Профессиональные компетенции	ПК-4.В/ПР Способен проводить разработку и настройку систем защиты информации и их компонентов
	ПК-4.В/ПР. 2 Умеет проводить разработку и настройку систем защиты информации и их компонентов

2. Требования НГТУ к планируемым результатам обучения, соотнесенным с индикаторами достижения компетенций

Таблица 2.1

Индикаторы достижения компетенций	Формы организации занятий
Результаты обучения	
ПК-2.В/ОУ. 2 Умеет осуществлять планирование и организацию работ по защите информации с учётом требований по информационной безопасности	
Обладает навыком осуществления планирования и организации работ по защите информации с учётом требований по информационной безопасности	Лекции; Практические занятия; Самостоятельная работа
ПК-3.В/КА. 2 Умеет оценивать уровень безопасности систем защиты информации и их компонентов	
Обладает навыком оценки уровня безопасности систем защиты информации и их компонентов	Лекции; Практические занятия; Самостоятельная работа
ПК-4.В/ПР. 2 Умеет проводить разработку и настройку систем защиты информации и их компонентов	
Обладает опытом разработки и настройки систем защиты информации и их компонентов	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура дисциплины

Таблица 3.1

Темы лекций	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций
Семестр: 9				
Дидактическая единица: Процессы создания и обеспечения информационной безопасности автоматизированных систем защиты информации (АСЗИ)				
1. Процессы жизненного цикла систем ГОСТ Р ИСО/МЭК 15288-2005 и программных средств ГОСТ Р ИСО/МЭК 12207. Системы безопасности комплексные и интегрированные. SSE-CMM модели проектирования систем безопасности.	2	0	0	ПК-2.В/ОУ. 2
2. Порядок создания АСЗИ. Общие положения ГОСТ Р 51583-2014. Стадии и этапы работ по созданию АСЗИ - ГОСТ 34.601. Содержание работ в части создания системы ЗИ.	2	0	0	ПК-2.В/ОУ. 2

3. Содержание и порядок выполнения работ по ЗИ о создаваемой АСЗИ. Требования по разработке документации на АСЗИ. Требования к управлению проектом ГОСТ Р 54869.	2	0	0	ПК-2.В/ОУ.2
4. Процесс анализа требований. Контекст задачи анализа требований. Классификация и специфицирование требований.	2	0	0	ПК-2.В/ОУ.2
5. Виды испытаний АСЗИ и общие требования к их проведению. Испытания АСЗИ на соответствие требованиям безопасности информации.	2	0	0	ПК-2.В/ОУ.2
6. Функциональная безопасность. Анализ методов и средств для Э/Э/ПЭ систем, связанных с безопасностью. Аттестация АСЗИ для подтверждения соответствия системы ЗИ АСЗИ.	2	0	0	ПК-2.В/ОУ.2
7. Формирование требований к системе ЗИ АСЗИ с учетом ГОСТ Р ИСО/МЭК 27005/МЭК 21827/МЭК27002.	2	0	0	ПК-2.В/ОУ.2
8. Разработка концепции АС с учетом ГОСТ Р ИСО/МЭК ТО 19791/МЭК 21827/МЭК27002/ МЭК ТО 15446.	2	0	0	ПК-3.В/КА.2
9. Состав работ на стадии "Техническое задание" в соответствии с требованиями ГОСТ 34.602 и " с учетом ГОСТ Р ИСО/МЭК ТО 19791/МЭК ТО 15446/МЭК 15408-1,2. Разработка (проектирование) системы ЗИ на стадиях создания АСЗИ в соответствии с требованиями ГОСТ 34.601.	2	0	0	ПК-3.В/КА.2
10. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на стадии "Эскизный проект".	2	0	0	ПК-3.В/КА.2
11. Этап "Разработка предварительных проектных решений по системе и ее частям". Определение функций системы ЗИ создаваемой (модернизируемой) АСЗИ, состава комплексов задач и отдельных задач, решаемых подсистемой ЗИ. Определение функций и параметров ТС и ПС системы ЗИ.	2	0	0	ПК-3.В/КА.2
12. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на этапе "Разработка документации на АС и ее части" стадии "Эскизный проект". Виды документов - по ГОСТ 34.201.	2	0	0	ПК-4.В/ПР.2
13. Состав работ стадии "Технический проект". Виды документов. Состав работ на стадии "Рабочая документация" в соответствии с требованиями РД 50-34.698-90.	2	0	0	ПК-4.В/ПР.2
14. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на этапе "Разработка документации на АС и ее части" стадии "Рабочая документация" с учетом ГОСТР ИСО/МЭК 15408-1,3.	2	0	0	ПК-4.В/ПР.2
15. Состав работ на стадии "Рабочая документация" этапе "Разработка и адаптация программ". Внедрение системы ЗИ АСЗИ.	2	0	0	ПК-4.В/ПР.2
16. Аттестация АСЗИ на соответствие требованиям безопасности информации. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ.	2	0	0	ПК-4.В/ПР.2

17. Состав работ стадии " Ввод в действие " с учетом ГОСТР ИСО/МЭК 15408-1,3/МЭК 18045.	2	0	0	ПК-4.В/ПР.2
18. Содержание и порядок выполнения работ по защите информации о создаваемой АСЗИ.	2	0	0	ПК-4.В/ПР.2

Темы практических занятий	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 9					
Дидактическая единица: Процессы создания и обеспечения информационной безопасности автоматизированных систем защиты информации (АСЗИ)					
1. Методы UML для моделирования и реализации парольной защиты приложений на языке VBA Access.	2	2	0	ПК-2.В/ОУ.2	Применение методов UML для проектирования и реализации системы парольной защиты приложений на VBA Access
2. Моделирование процессов реализации сетевого анализа с использованием система имитационного моделирования ARENA.	4	4	0	ПК-2.В/ОУ.2	Использование системы имитационного моделирования ARENA для анализа и оптимизации сетевых процессов
3. Моделирование процессов реализации угроз непосредственного и удаленного доступа к элементам ИКТС.	4	4	0	ПК-3.В/КА.2	Анализ и моделирование угроз прямого и удаленного доступа к компонентам ИКТС
4. Моделирование процессов реализации нескольких угроз непосредственного и удаленного доступа к элементам ИКТС.	4	4	0	ПК-3.В/КА.2	Анализ и моделирование процессов реализации различных угроз прямого и удаленного доступа к ИКТС
5. Анализа реализации угроз непосредственного и удаленного доступа к элементам ИТКС.	2	2	0	ПК-4.В/ПР.2	Анализ реализации угроз прямого и удаленного доступа к элементам информационных технологий и коммуникационных систем (ИТКС)
6. Анализа реализации нескольких угроз непосредственного и удаленного доступа к элементам ИТКС.	2	2	0	ПК-4.В/ПР.2	Анализ реализации множества угроз прямого и удаленного доступа к элементам информационно-технологических и коммуникационных систем (ИТКС)

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Методы UML для моделирования и реализации парольной защиты приложений на языке VBA Access.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу

2	Моделирование процессов реализации сетевого анализа с использованием система имитационного моделирования ARENA.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
3	Моделирование процессов реализации угроз непосредственного и удаленного доступа к элементам ИКТС.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
4	Моделирование процессов реализации нескольких угроз непосредственного и удаленного доступа к элементам ИКТС.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
5	Анализа реализации угроз непосредственного и удаленного доступа к элементам ИТКС.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
6	Анализа реализации нескольких угроз непосредственного и удаленного доступа к элементам ИТКС.	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 9				
1	Подготовка к занятиям	ПК-2.В/ОУ.2,ПК-3.В/КА.2,ПК-4.В/ПР.2	24	0
: Зырянов С. А. Информационная безопасность в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т.- Новосибирск, [2018].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000237649.- Загл. с экрана.				
2	Дополнительная учебная деятельность	ПК-2.В/ОУ.2,ПК-3.В/КА.2,ПК-4.В/ПР.2	40	10
: Зырянов С. А. Информационная безопасность в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т.- Новосибирск, [2018].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000237649.- Загл. с экрана.				
3	Подготовка к аттестации	ПК-2.В/ОУ.2,ПК-3.В/КА.2,ПК-4.В/ПР.2	40	10
: Зырянов С. А. Информационная безопасность в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т.- Новосибирск, [2018].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000237649.- Загл. с экрана.				

3.3 Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 3.4).

Таблица 3.4

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Среда электронного обучения НГТУ

Консультирование	e-mail; Среда электронного обучения НГТУ
Контроль	Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ

4. Правила аттестации обучающихся по дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 4.1.

Таблица 4.1

Оцениваемые виды деятельности обучающихся	**Мин. балл**	**Максимальный балл**
Семестр: 9		
Практические занятия:	30	60
Экзамен:	20	40

В таблице 4.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 4.2

Коды компетенций	**Индикаторы достижения компетенций**	**Формы контроля**
		Экзамен
ПК-2.В/ОУ	ПК-2.В/ОУ 2. Умеет осуществлять планирование и организацию работ по защите информации с учётом требований по информационной безопасности	+
ПК-3.В/КА	ПК-3.В/КА 2. Умеет оценивать уровень безопасности систем защиты информации и их компонентов	+
ПК-4.В/ПР	ПК-4.В/ПР 2. Умеет проводить разработку и настройку систем защиты информации и их компонентов	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

5. Литература

Основная литература

1. Нефедов, В. С. Безопасность прикладных информационных технологий и систем : учебное пособие / В. С. Нефедов. — 2-е изд. — Москва : РТУ МИРЭА, 2025. — 113 с. — ISBN 978-5-7339-2570-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504831 (дата обращения: 13.08.2026). — Режим доступа: для авториз. пользователей.

Дополнительная литература

1. Методика построения модели безопасности автоматизированных систем [Программные продукты и системы, 2 (98), 2012, стр. -] - Текст : электронный. - URL: https://znanium.com/catalog/product/463119 (дата обращения: 11.08.2026). – Режим доступа: по подписке.

Интернет-ресурсы

1. Банк данных угроз безопасности информации : [сайт] / ФСТЭК России. – URL: https://bdu.fstec.ru/threat (дата обращения: 06.07.2026). – Текст : электронный.

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Зырянов С. А. Информационная безопасность в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т.- Новосибирск, [2018].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000237649.- Загл. с экрана.

2. Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т.- Новосибирск, [2014].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798.- Загл. с экрана.

6.2 Специализированное программное обеспечение

1 Система управления базами данных (СУБД) Microsoft Access

2 ПО для виртуализации Vmware, Inc. Vmware

3 Имитационное моделирование бизнес-процессов Rockwell Software CИМ Arena

4 Операционная система Open Source Software Операционные системы семества LINUX

5 ОС для применения на серверах Microsoft Windows

6.3 Информационные технологии

При осуществлении образовательного процесса по дисциплине применяются элементы дистанционных образовательных технологий, а также синхронного и асинхронного взаимодействия в электронной информационно-образовательной среды НГТУ.

7. Материально-техническое обеспечение

Лабораторный стенд

№	Наименование	Назначение
1	Компьютерный класс№4	Компьютерный класс для изучения программ и программно-аппаратных комплексов по защите информации