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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Томилов И. Н.

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защищенные информационные системы

Образовательная программа: 10.04.01 Информационная безопасность, магистерская программа: Методы и средства обеспечения технической защиты информации

Курс: 2, семестр : 3

Факультет автоматики и вычислительной техники,

		Семестр
№	Вид деятельности	3
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	44
4	Лекции, час.	18
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	0
8	из них практической подготовки, час.	7
9	Аттестация, час.	2
10	Консультации, час.	6
11	Самостоятельная работа, час.	100
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): 10.04.01 Информационная безопасность

ФГОС введен в действие приказом №1455 от 26.11.2020 г. , дата утверждения: 18.02.2021 г.

Место дисциплины в структуре учебного плана: Блок 1, обязательная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.04.01 Информационная безопасность

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
Общепрофессиональные компетенции	ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
	ОПК-1. 2 владеет навыками участия в разработке системы обеспечения информационной безопасности объекта
	ОПК-1. 3 умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от утечки по техническим каналам
	ОПК-1. 4 умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от несанкционированного доступа

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

Таблица 2.1

Индикаторы достижения компетенций / Результаты обучения	Формы организации занятий
ОПК-1. 2 владеет навыками участия в разработке системы обеспечения информационной безопасности объекта	
Способен участвовать в разработке системы обеспечения информационной безопасности объекта	Лекции; Лабораторные работы; Самостоятельная работа
Готов решать типовые задачи разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	Лекции; Лабораторные работы; Самостоятельная работа
ОПК-1. 3 умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от утечки по техническим каналам	
Способен проектировать информационные системы с учетом различных технологий защиты от утечки данных по техническим каналам	Лекции; Лабораторные работы;
ОПК-1. 4 умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от несанкционированного доступа	
Готов проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от несанкционированного доступа	Лекции; Лабораторные работы; 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: 3				
Дидактическая единица: Информационная система как объект защиты				
1. Информационная система как объект защиты	6	0	0	ОПК-1.2
Дидактическая единица: Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем				
2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	6	0	0	ОПК-1.2,ОПК-1.3,ОПК-1.4

Дидактическая единица: Организационно-технические меры по реализации основных требований и построению системы информационной безопасности				
3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	6	0	0	ОПК-1.2,ОПК-1.4

Темы лабораторных работ	**Часы**	**Из них в форме практ. подг., час.**	**Активные формы, час.**	**Индикаторы достижения компетенций**	**Учебная деятельность**
Семестр: 3					
Дидактическая единица: Информационная система как объект защиты					
1. Информационная система как объект защиты	6	2	0	ОПК-1.2	Эволюция архитектур информационных систем. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз.
Дидактическая единица: Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем					
2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	6	2	0	ОПК-1.4	Общие требования построения защищенной информационной системы. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Требования к подсистеме аутентификации и управления доступом. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды. Требования к средствам построения защищенных сетей и управления безопасностью.
Дидактическая единица: Организационно-технические меры по реализации основных требований и построению системы информационной безопасности					

3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	6	3	0	ОПК-1.2,ОПК-1.3,ОПК-1.4	Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»: методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели. Протокол формирования защищенного туннеля на канальном уровне. Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации. Технические решения по защите от вредоносного кода. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Информационная система как объект защиты	Лб	Выполняет следующие виды работ: студенты создают модели нарушителя и угроз, проводят анализ рисков.
2	Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем	Лб	Выполняет следующие виды работ: студенты должны сформулировать: Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Требования к подсистеме аутентификации и управления доступом. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Требования к подсистемам резервирования/восстановления информации, контроля эталонного состояния информации и рабочей среды. Требования к средствам построения защищенных сетей и управления безопасностью.
3	Организационно-технические меры по реализации основных требований и построению системы информационной безопасности	Лб	Выполняет следующие виды работ: студенты создают многоуровневую модель защиты в информационной системе на архитектуре «клиент-сервер».

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 3				
1	Подготовка к занятиям	ОПК-1.2,ОПК-1.4	60	4
: Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012				
2	Дополнительная учебная деятельность	ОПК-1.2	40	2
: Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012				

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; Социальные сети; Среда электронного обучения НГТУ
Консультирование	e-mail; Социальные сети; 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: 3		
Лабораторная:	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
ОПК-1	ОПК-1 2. владеет навыками участия в разработке системы обеспечения информационной безопасности объекта		+

	ОПК-1 3. умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от утечки по техническим каналам	+
	ОПК-1 4. умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от несанкционированного доступа	+

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

5. Литература

Основная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 22.09.2021). – Режим доступа: по подписке.

2. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021744 (дата обращения: 22.09.2021). – Режим доступа: по подписке.

3. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://znanium.com/catalog/product/1082470 (дата обращения: 22.09.2021). – Режим доступа: по подписке.

Дополнительная литература

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 22.09.2021). – Режим доступа: по подписке.

2. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 22.09.2021). – Режим доступа: по подписке.

Интернет-ресурсы

1. Федеральная служба по техническому и экспортному контролю : сайт. – URL: https://fstec.ru/ (дата обращения: 03.03.2021). – Текст : электронный.

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Дронова Г. А. Управление информационной безопасностью : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 23, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234012

6.2 Специализированное программное обеспечение

1 СКЗИ для защиты передачи информации Код безопасности АПКШ Континент, Континент TLS

2 сканер безопасности Сканер-ВС Сканер-ВС

3 Межсетевое экранирование Ideco Ideco UTM
4 Межсетевое экранирование UserGate UserGate UTM

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

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)