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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН ФЭН
д.т.н. Русина А. Г.

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2026
Владелец: д.т.н. Русина А. Г.
Срок действия: не ограничен
Адрес хранения электронного документа:
https://www.nstu.ru/university/info/sveden/education

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность в корпоративной сфере. Продвинутый уровень (для продолжающих)

Образовательная программа: 13.04.02 Электроэнергетика и электротехника, магистерская программа: Техника и электрофизика высоких напряжений

Курс: 1, семестр : 1

Факультет энергетики,

		Семестр
№	**Вид деятельности**	**1**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	40
4	Лекции, час.	18
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	16
8	из них практической подготовки, час.	18
9	Аттестация, час.	2
10	Консультации, час.	2
11	Самостоятельная работа, час.	68
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	Р
13	Вид аттестации	3

Новосибирск 2026

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 13.04.02 Электроэнергетика и электротехника

ФГОС введен в действие приказом №147 от 28.02.2018 г. , дата утверждения: 22.03.2018 г.

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

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 13.04.02 Электроэнергетика и электротехника

Рабочая программа обсуждена на заседании кафедры

ЗИ, 31.08.2026

Утверждена на совете факультета энергетики, протокол № 8 от 31.08.2026

Заведующий кафедрой:

доцент, к.т.н. Иванов А. В.

Ответственный за образовательную программу:

заведующий кафедрой Трофимов А. С.

1. Внешние требования

Таблица 1.1

Группа	Компетенции
	Индикаторы достижения компетенций
Профессиональные компетенции	ПК-3.В/ПР Способен формулировать технические задания и использовать средства автоматизации при проектировании объектов профессиональной деятельности
	ПК-3.В/ПР. 3 Использует средства автоматизации при проектировании
Универсальные компетенции	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
	УК-4. 3 Использует современные информационно-коммуникативные средства для коммуникации

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

Таблица 2.1

Индикаторы достижения компетенций	Формы организации занятий
Результаты обучения	
ПК-3.В/ПР. 3 Использует средства автоматизации при проектировании	
умеет использовать средства автоматизации при проектировании	Лекции; Лабораторные работы; Самостоятельная работа
УК-4. 3 Использует современные информационно-коммуникативные средства для коммуникации	
умеет использовать современные информационно-коммуникативные средства для коммуникации	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	Учебная деятельность
Семестр: 1					
Дидактическая единица: Основы информационной безопасности и защиты информации					
1. Классификация информационных систем. Правовые, нормативные и методические документы, национальные стандарты в области защиты информации	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
2. Категорирование информационных систем	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
3. Моделирование угроз безопасности	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
4. Требования по защите информации	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
5. Базовые средства защиты информации	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
6. Экспертные средства защиты информации	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	

7. Принципы организации мониторинга безопасности	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
8. Основные процессы информационной безопасности	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	
9. Защита типовой инфраструктуры	2	0	0	ПК-3.В/ПР.3 ,УК-4.3	

Темы лабораторных работ	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 1					
Дидактическая единица: Основы информационной безопасности и защиты информации					
1. Классификация информационных систем. Правовые, нормативные и методические документы, национальные стандарты в области защиты информации	2	2	0	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы, связанные с классификацией информационных систем. Дается понятие информационной системе. Приводятся нормативно-правовые акты, связанные с защитой информации в государственных и муниципальных информационных системах, информационных системах персональных данных, автоматизированных системах управления производственными и технологическими процессами, объектах критических информационных инфраструктур Российской Федерации.

2. Категорирование информационных систем	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	Рассматриваются процедуры определения класса защищенности государственных и муниципальных информационных систем, автоматизированных систем управления производственными и технологическими процессами, уровня защищенности персональных данных и категории значимости объекта критической информационной инфраструктуры Российской Федерации. Приводятся нормативно-правовые акты, регламентирующие процедуру категоризации.
3. Моделирование угроз безопасности	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы, связанные с моделирование угроз безопасности информации. Рассматривается Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). Приводится описание процедур, необходимых для проведения моделирования угроз безопасности информации.
4. Требования по защите информации	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы, связанные с мерами защиты информации, определяемые регуляторами в области защиты информации. Разбираются требования Федеральной службой по техническому и экспортному контролю. Рассматриваются требования Федеральной службы безопасности в отношении применения средств криптографической защиты информации.

5. Базовые средства защиты информации	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы. связанные с видами и принципами функционирования базовых средств защиты информации. Рассмотрены такие системы как средства защиты информации от несанкционированного доступа, системы обнаружения и предотвращения вторжений, межсетевые экраны, антивирусные средства защиты информации, средства криптографической защиты информации, электронные подписи, решения класса EDR и XDR, а также сканеры уязвимостей.
6. Экспертные средства защиты информации	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы. связанные с видами и принципами функционирования экспертных средств защиты информации. Рассмотрены такие системы как песочницы (sandbox), системы предотвращения утечек конфиденциальной информации, SIEM системы, системы класса UBA и UEBA, системы класса IRP и SOAR, а также системы Threat Intelligence.

7. Принципы организации мониторинга безопасности	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы, связанные с построением и сопровождением процесса мониторинга информационной безопасности организации. Даются понятия реактивной и проактивной безопасности. Дается определение центра мониторинга информационной безопасности (Security Operation Center). Приводятся цели и задачи процесса, типовые формы реализации, возможные вариации технических и организационных решений.
8. Основные процессы информационной безопасности	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются вопросы, связанные с реализацией процессов информационной безопасности верхнего уровня. Даются определения процессов Threat Intelligence, Threat Hunting, управление уязвимостями, реагирование на инциденты информационной безопасности. Приводятся цели и задачи процессов, типовые формы реализации, возможные вариации технических и организационных решений при внедрении приведенных процессов.

9. Защита типовой инфраструктуры	2	2	2	ПК-3.В/ПР.3 ,УК-4.3	В данной теме рассматриваются типовые технические решения для обеспечения информационной безопасности на периметре и внутри сети организации. Даются цели и задачи, достигаемые применением тех или иных решений. Приводятся типовые формы реализации, возможные пути решения задач по обеспечению технической безопасности информации в организации.

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Классификация информационных систем. Правовые, нормативные и методические документы, национальные стандарты в области защиты информации	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
2	Категорирование информационных систем	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
3	Моделирование угроз безопасности	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
4	Требования по защите информации	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
5	Базовые средства защиты информации	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
6	Экспертные средства защиты информации	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
7	Принципы организации мониторинга безопасности	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
8	Основные процессы информационной безопасности	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
9	Защита типовой инфраструктуры	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 1				
1	РГЗ/Реферат	ПК-3.В/ПР.3,УК-4.3	20	0
: Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1359091 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=375641 - Загл. с экрана.				
2	Подготовка к занятиям	ПК-3.В/ПР.3,УК-4.3	10	0
: Нуждина Л. Е. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебно-методическое пособие / Л. Е. Нуждина ; Новосиб. гос. техн. ун-т.- Новосибирск, [2013].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000183569.- Загл. с экрана.				
3	Дополнительная учебная деятельность	ПК-3.В/ПР.3,УК-4.3	26	0
: Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=445102 - Загл. с экрана. Нуждина Л. Е. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебно-методическое пособие / Л. Е. Нуждина ; Новосиб. гос. техн. ун-т.- Новосибирск, [2013].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000183569.- Загл. с экрана.				
4	Подготовка к аттестации	ПК-3.В/ПР.3,УК-4.3	12	2
: Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1359091 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=375641 - Загл. с экрана. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=445102 - Загл. с экрана. Нуждина Л. Е. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебно-методическое пособие / Л. Е. Нуждина ; Новосиб. гос. техн. ун-т.- Новосибирск, [2013].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000183569.- 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: 1		
Лабораторная:	25	50
РГЗ/Реферат:	15	30
Зачет:	10	20

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

Таблица 4.2

Коды компетенций	**Индикаторы достижения компетенций**	**Формы контроля**	
		Защита РГЗ/Р	**Зачет**
ПК-3.В/ПР	ПК-3.В/ПР 3. Использует средства автоматизации при проектировании	+	+
УК-4	УК-4 3. Использует современные информационно-коммуникативные средства для коммуникации	+	+

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

5. Литература

Основная литература

1. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=445102 - Загл. с экрана.

2. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=426504 - Загл. с экрана.

Дополнительная литература

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./НовиковВ.К. - Москва : Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст : электронный. - URL: https://znanium.ru/catalog/product/536932 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=67242 - Загл. с экрана.

Интернет-ресурсы

1. Организационно-правовое обеспечение информационной безопасности. – Текст : электронный // Хабр = Habr : сайт. – URL: https://habr.com/ru/articles/741686/ (дата обращения: 18.08.2026).

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Нуждина Л. Е. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебно-методическое пособие / Л. Е. Нуждина ; Новосиб. гос. техн. ун-т.- Новосибирск, [2013].- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000183569.- Загл. с экрана.

2. Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1359091 (дата обращения: 10.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=375641 - Загл. с экрана.

6.2 Специализированное программное обеспечение

1 ОС для применения на серверах Microsoft Windows

2 Пакет офисных приложений Microsoft Office

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

Компьютерный класс

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	демонстрация учебных материалов
2	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	выполнение практических работ