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
Расследование инцидентов информационной безопасности

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.	76
4	Лекции, час.	36
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.	6
9	Аттестация, час.	2
10	Консультации, час.	20
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): 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, формируемая участниками образовательных отношений, по выбору студента

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
Профессиональные компетенции	ПК-3.В/НИ Способен проводить расследования компьютерных преступлений
	ПК-3.В/НИ. 1 умеет анализировать данные, связанные с компьютерным преступлением
	ПК-3.В/НИ. 2 знает инструменты для проведения расследования киберинцидентов

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/НИ. 1 умеет анализировать данные, связанные с компьютерным преступлением	
Быть готовым анализировать данные, связанные с компьютерным преступлением	Лекции; Лабораторные работы; Самостоятельная работа
ПК-3.В/НИ. 2 знает инструменты для проведения расследования киберинцидентов	
Понимать и применять инструменты для проведения расследования киберинцидентов	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: 3					
Дидактическая единица: Стандартизация в области управления инцидентами ИБ. Базовые вопросы управления инцидентами ИБ					
1. Введение.	2	0	0	ПК-3.В/НИ. 2	Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний.

2. Нормативная база управления инцидентами ИБ	4	2	0	ПК-3.В/НИ.2	Существующие стандарты и методологии по управлению инцидентами ИБ: их отличия, сильные и слабые стороны. История развития. ISO/IEC 27035:2011 - управление инцидентами ИБ. ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
3. Система управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Событие и инцидент ИБ. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Цели и задачи управления инцидентами ИБ. Система управления инцидентами ИБ (СУИИБ).
4. Процесс управления инцидентами ИБ	6	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИИБ). Важность процесса управления инцидентами ИБ с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Связи с другими процессами СУИБ. Обязательные этапы процесса. Планирование и подготовка процесса. Внедрение процесса. Использование СУИИБ. Анализ процесса. Улучшение процесса.

5. Обнаружение и обработка событий и инцидентов ИБ	4	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Обнаружение событий ИБ и инцидентов ИБ и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Первая оценка и предварительное решение по событию ИБ. Вторая оценка и подтверждение инцидента ИБ.
6. Реагирование на инциденты ИБ	4	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Немедленное реагирование на инцидент ИБ. Контролируемость инцидента ИБ. Последующее реагирование на инцидент ИБ. Антикризисные действия. Правовая экспертиза инцидентов ИБ. Передача информации. Расширение области принятия решений. Регистрация деятельности и контроль за внесением изменений. Техническая поддержка реагирования на инциденты ИБ.
Дидактическая единица: Документация СУИИБ. Кадровые и технические вопросы при управлении инцидентами ИБ					
7. Программа управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Основные цели. Структура. Содержание. Другие документы: формы регистрации инцидентов, регламенты сбора свидетельств инцидентов ИБ и т.п.
8. Группа реагирования на инциденты ИБ	4	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Цели, задачи. Состав группы. Понятие роли. Использование ролевого принципа в рамках СУИИБ. Преимущества использования ролевого принципа. Ролевая структура СУИИБ (основные и дополнительные роли).
9. Политика управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Основные цели. Структура. Содержание.
10. Обеспечение осведомленности и обучение в области инцидентов ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Обеспечение осведомленности и обучение в области инцидентов ИБ

11. Технические вопросы при управлении инцидентами ИБ	4	4	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Сохранение доказательств инцидента ИБ. Средства управления событиями ИБ.

Темы лабораторных работ	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 3					
Дидактическая единица: Стандартизация в области управления инцидентами ИБ. Базовые вопросы управления инцидентами ИБ					
1. Нормативная база управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.2	Существующие стандарты и методологии по управлению инцидентами ИБ: их отличия, сильные и слабые стороны. История развития. ISO/IEC 27035:2011 - управление инцидентами ИБ. ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
2. Система управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.2	Событие и инцидент ИБ. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Цели и задачи управления инцидентами ИБ. Система управления инцидентами ИБ (СУИИБ).

3. Процесс управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИИБ). Важность процесса управления инцидентами ИБ с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Связи с другими процессами СУИБ. Обязательные этапы процесса. Планирование и подготовка процесса. Внедрение процесса. Использование СУИИБ. Анализ процесса. Улучшение процесса.
4. Обнаружение и обработка событий и инцидентов ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Обнаружение событий ИБ и инцидентов ИБ и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Первая оценка и предварительное решение по событию ИБ. Вторая оценка и подтверждение инцидента ИБ.
5. Реагирование на инциденты ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Немедленное реагирование на инцидент ИБ. Контролируемость инцидента ИБ. Последующее реагирование на инцидент ИБ. Антикризисные действия. Правовая экспертиза инцидентов ИБ. Передача информации. Расширение области принятия решений. Регистрация деятельности и контроль за внесением изменений. Техническая поддержка реагирования на инциденты ИБ.

Дидактическая единица: Документация СУИИБ. Кадровые и технические вопросы при управлении инцидентами ИБ					
6. Программа управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Основные цели. Структура. Содержание. Другие документы: формы регистрации инцидентов, регламенты сбора свидетельств инцидентов ИБ и т.п.
7. Группа реагирования на инциденты ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Цели, задачи. Состав группы. Понятие роли. Использование ролевого принципа в рамках СУИИБ. Преимущества использования ролевого принципа. Ролевая структура СУИИБ (основные и дополнительные роли).
8. Политика управления инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Основные цели. Структура. Содержание.
9. Технические вопросы при управлении инцидентами ИБ	2	0	0	ПК-3.В/НИ.1,ПК-3.В/НИ.2	Сохранение доказательств инцидента ИБ. Средства управления событиями ИБ.

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Нормативная база управления инцидентами ИБ	Л	Выполняет следующие виды работ: студенты изучают стандарты и методологии по управлению инцидентами ИБ.
2	Технические вопросы при управлении инцидентами ИБ	Л	Выполняет следующие виды работ: создание средств управления событиями ИБ.

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 3				
1	РГЗ/Реферат	ПК-3.В/НИ.1,ПК-3.В/НИ.2	20	16
Нормативная база управления инцидентами ИБ.: 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. Зырянов С. А. Основы информационной безопасности в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2021]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000243905. - Загл. с экрана.			

2	Подготовка к занятиям	ПК-3.В/НИ.1,ПК-3.В/НИ.2	30	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.				
3	Дополнительная учебная деятельность	ПК-3.В/НИ.1,ПК-3.В/НИ.2	10	4
: Зырянов С. А. Основы информационной безопасности в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2021]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000243905. - Загл. с экрана.				
4	Подготовка к аттестации	ПК-3.В/НИ.1,ПК-3.В/НИ.2	8	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.				

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; 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: 3		
Лабораторная:	30	60
РГЗ/Реферат:	10	20
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/НИ	ПК-3.В/НИ 1. умеет анализировать данные, связанные с компьютерным преступлением	+	+
	ПК-3.В/НИ 2. знает инструменты для проведения расследования киберинцидентов		+

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

5. Литература

Основная литература

1. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889 (дата обращения: 12.12.2023). — Режим доступа: для авториз. пользователей.

2. Гришина, Н. В. Основы управления информационной безопасностью : учебно-методическое пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 99 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-110048-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1859951 (дата обращения: 12.12.2023). – Режим доступа: по подписке.

Дополнительная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/document?id=431346#bib (дата обращения: 12.12.2023). – Режим доступа: по подписке.

2. Комплексные системы защиты информации на предприятиях : учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома : КГУ, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/201884 (дата обращения: 12.12.2023). — Режим доступа: для авториз. пользователей.

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. Зырянов С. А. Основы информационной безопасности в автоматизированных системах [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2021]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000243905. - Загл. с экрана.

2. 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.

6.2 Специализированное программное обеспечение

1 ПО Форензики AutoPsy Digital Forensics AutoPsy
2 Платформа учета инцидентов ИБ StrangeBee TheHive
3 ПО форезнзики Volatility Volatility

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)	Для проведения лекционных занятий

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Для проведения лабораторных работ