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
Расследование инцидентов информационной безопасности

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)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	74
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.	18
11	Самостоятельная работа, час.	70
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	
13	Вид аттестации	3

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-3.В/КА Способен осуществлять контрольно-аналитическую дея-тельность и оценивать уровень безопасности систем защиты информации и их компонентов
	ПК-3.В/КА. 1 Владеет навыками реализации контрольно-аналитической деятельности и оценки уровня безопасности систем защиты информации и их компонентов
	ПК-3.В/КА. 3 Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности

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/КА. 1 Владеет навыками реализации контрольно-аналитической деятельности и оценки уровня безопасности систем защиты информации и их компонентов	
Умеет реализовывать контрольно-аналитическую деятельность и оценку уровня безопасности систем защиты информации и их компонентов	Практические занятия; Самостоятельная работа
ПК-3.В/КА. 3 Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности	
Владеет информацией о нормативно-методической базе по осуществлению контрольно-аналитической деятельности	Лекции; 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: 9					
Дидактическая единица: Комплексный подход к расследованию инцидентов информационной безопасности					
1. Общие понятия	4	0	0	ПК-3.В/КА. 3	Лекционные занятия
2. Юридические и организационные аспекты расследований инцидентов информационной безопасности	4	0	0	ПК-3.В/КА. 3	Лекционные занятия
3. Начало работы с инцидентами	4	0	0	ПК-3.В/КА. 3	Лекционные занятия
4. Форензика оперативной памяти	4	0	0	ПК-3.В/КА. 3	Лекционные занятия
5. Форензика дисков	4	0	0	ПК-3.В/КА. 3	Лекционные занятия

6. Системное журналирование	4	0	0	ПК-3.В/КА.3	Лекционные занятия
7. Анализ активности приложений	4	0	0	ПК-3.В/КА.3	Лекционные занятия
8. Анализ активности пользователя	4	0	0	ПК-3.В/КА.3	Лекционные занятия
9. Анализ активности вредоносного программного обеспечения	4	0	0	ПК-3.В/КА.3	Лекционные занятия

Темы практических занятий	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 9					
Дидактическая единица: Комплексный подход к расследованию инцидентов информационной безопасности					
1. Поиск вредоносной активности в сетевом трафике	4	4	0	ПК-3.В/КА.1	Исследование сетевого трафика для поиска индикаторов компометации инфраструктуры
2. Анализ событий журналов Windows	4	4	0	ПК-3.В/КА.1	Исследование журналов событий: анализ, оценка масштаба инцидента и определение ущерба
3. Снятие дампа ОП, анализ дампа ОП	4	4	0	ПК-3.В/КА.1	Исследование оперативной памяти для поиска индикаторов компрометации
4. Снятие дампа ЖМД, сбор артефактов с ЖМД, анализ журналов событий Windows	4	4	0	ПК-3.В/КА.1	Исследование постоянной памяти для поиска индикаторов компрометации
5. Анализ журналов ОС Linux	2	2	0	ПК-3.В/КА.1	Исследование журналов событий: анализ, оценка масштаба инцидента и определение ущерба

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Поиск вредоносной активности в сетевом трафике	Пр	Выполняет следующие виды работ: выполняет практическое задание; оформляет отчет; защищает практическое задание
2	Анализ событий журналов Windows	Пр	Выполняет следующие виды работ: выполняет практическое задание; оформляет отчет; защищает практическое задание
3	Снятие дампа ОП, анализ дампа ОП	Пр	Выполняет следующие виды работ: выполняет практическое задание; оформляет отчет; защищает практическое задание

4	Снятие дампа ЖМД, сбор артефактов с ЖМД, анализ журналов событий Windows	Пр	Выполняет следующие виды работ: выполняет практическое задание; оформляет отчет; защищает практическое задание
5	Анализ журналов ОС Linux	Пр	Выполняет следующие виды работ: выполняет практическое задание; оформляет отчет; защищает практическое задание

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-3.В/КА.1,ПК-3.В/КА.3	20	8
: Жукова М. Н. Управление информационной безопасностью : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - Ч. 2 : Управление инцидентами информационной безопасности. - 100 с. - URL: https://znanium.com/catalog/product/463061 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.				
2	Дополнительная учебная деятельность	ПК-3.В/КА.1,ПК-3.В/КА.3	20	0
: Жукова М. Н. Управление информационной безопасностью : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - Ч. 2 : Управление инцидентами информационной безопасности. - 100 с. - URL: https://znanium.com/catalog/product/463061 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.				
3	Подготовка к аттестации	ПК-3.В/КА.1,ПК-3.В/КА.3	30	10
: Жукова М. Н. Управление информационной безопасностью : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - Ч. 2 : Управление инцидентами информационной безопасности. - 100 с. - URL: https://znanium.com/catalog/product/463061 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.				

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:	40	80
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	
			Зачет
ПК-3.В/КА	ПК-3.В/КА 1. Владеет навыками реализации контрольно-аналитической деятельности и оценки уровня безопасности систем защиты информации и их компонентов		+
	ПК-3.В/КА 3. Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности		+

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

5. Литература

Основная литература

1. Островская С. Криминалистика компьютерной памяти на практике: как эффективно анализировать оперативную память : практическое рук-во / С. Островская, О. Скулкин ; пер. с англ. А. А. Слинкина. - Москва : ДМК Пресс, 2023. - 258 с. - ISBN 978-5-93700-157-3. - URL: https://znanium.ru/catalog/product/2109510 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

2. Ручкин В. Н. Современные компьютерные технологии и криминалистика : учеб. пособие / В. Н. Ручкин, В. В. Фомин. - Рязань : Академия ФСИН России, 2019. - 101 с. - ISBN 978-5-7743-0920-7. - URL: https://znanium.ru/catalog/product/1254336 (дата обращения: 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

Дополнительная литература

1. Милославская Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учеб. пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд. - Москва : Гор. линия-Телеком, 2016. - 170 с. - ISBN 978-5-9912-0363-0. - URL: https://znanium.ru/catalog/product/560782 (дата обращения 25.06.2026). – Режим доступа: по подписке. - Текст : электронный.

2. Целых А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учеб. пособие / А. Н. Целых, Э. М. Котов ; Южный федеральный университет. - Ростов-на-Дону : Изд-во Южного федерального университета, 2023. - 116 с. - ISBN 978-5-9275-4515-5. - URL: https://znanium.ru/catalog/product/2146710 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

Интернет-ресурсы

1. Компьютерная форензика: ключевые инструменты и методы работы : [статья]. – Текст : электронный // SecurityLab.ru : сайт. – Раздел сайта «Нейро синапс». – URL: https://www.securitylab.ru/blog/personal/Neurosinaps/354344.php?ysclid=mqufw3cq7h894578747 (дата обращения: 02.07.2026).

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Жукова М. Н. Управление информационной безопасностью : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - Ч. 2 : Управление инцидентами информационной безопасности. - 100 с. - URL: https://znanium.com/catalog/product/463061 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

6.2 Специализированное программное обеспечение

1 ПО для виртуализации Vmware, Inc. Vmware

2 Операционная система Open Source Software Операционные системы семества LINUX

3 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