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
Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей

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.	0
6	Лабораторные занятия, час.	18
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-3.В/КА Способен осуществлять контрольно-аналитическую дея-тельность и оценивать уровень безопасности систем защиты информации и их компонентов
	ПК-3.В/КА. 3 Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности
Профессиональные компетенции	ПК-4.В/ПР Способен проводить разработку и настройку систем защиты информации и их компонентов
	ПК-4.В/ПР. 3 Знает принципы построения систем защиты информации, включая настройку таких систем и их компонентов
Профессиональные компетенции	ПК-5.В/НИ Способен проводить исследования защищенности информации от утечек по техническим каналам и анализ их результатов
	ПК-5.В/НИ. 2 Умеет производить исследования по оценке защищённости информации от утечек по техническим каналам и осуществлять анализ их результатов

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. 3 Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности	
Владеет информацией о нормативно-методической базе по осуществлению контрольно-аналитической деятельности	Лекции; Самостоятельная работа
ПК-4.В/ПР. 3 Знает принципы построения систем защиты информации, включая настройку таких систем и их компонентов	
Владеет информацией о принципах построения систем защиты информации, включая настройку таких систем и их компонентов	Лекции; Самостоятельная работа
ПК-5.В/НИ. 2 Умеет производить исследования по оценке защищённости информации от утечек по техническим каналам и осуществлять анализ их результатов	
Имеет опыт по проведению исследования по оценке защищённости информации от утечек по техническим каналам и осуществлять анализ их результатов	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: 9				
Дидактическая единица: Мониторинг информационной безопасности: концепции, методы и инструменты для обеспечения защиты систем и данных				
1. Введение в мониторинг информационной безопасности	2	0	0	ПК-4.В/ПР.3

2. Правовые и этические аспекты мониторинга информационной безопасности	2	0	0	ПК-3.В/КА.3
3. Основные понятия мониторинга информационной безопасности	2	0	0	ПК-4.В/ПР.3
4. Методы агрегации, нормализации и корреляции журналов событий	2	0	0	ПК-3.В/КА.3
5. Средства мониторинга информационной безопасности	2	0	0	ПК-3.В/КА.3
6. Мониторинг Linux и Windows систем	2	0	0	ПК-4.В/ПР.3
7. Сетевой анализ трафика и системы обнаружения вторжений нового поколения	2	0	0	ПК-3.В/КА.3
8. Мониторинг безопасности контейнеризированных сред и оркестраторов	2	0	0	ПК-4.В/ПР.3
9. Использование фреймворка MITRE ATT&CK для проектирования правил мониторинга. Обнаружение сложных угроз	2	0	0	ПК-4.В/ПР.3
10. Архитектура систем мониторинга информационной безопасности	2	0	0	ПК-4.В/ПР.3
11. Особенности мониторинга промышленных (ICS/SCADA) и IoT-сетей	2	0	0	ПК-4.В/ПР.3
12. Интеграция данных об угрозах (Threat Intelligence) в системы мониторинга	2	0	0	ПК-4.В/ПР.3
13. Автоматизация процессов мониторинга и первичного реагирования	2	0	0	ПК-4.В/ПР.3
14. Мониторинг безопасности облачных и гибридных инфраструктур	2	0	0	ПК-4.В/ПР.3
15. Мониторинг инсайдерских угроз и поведенческий анализ	2	0	0	ПК-4.В/ПР.3
16. Базовые метрики SOC	2	0	0	ПК-4.В/ПР.3
17. Модели зрелости SOC	2	0	0	ПК-4.В/ПР.3
18. Управление знаниями и базами знаний в системах мониторинга	2	0	0	ПК-4.В/ПР.3

Темы лабораторных работ	**Часы**	**Из них в форме практ. подг., час.**	**Активные формы, час.**	**Индикаторы достижения компетенций**	**Учебная деятельность**
Семестр: 9					
Дидактическая единица: Мониторинг информационной безопасности: концепции, методы и инструменты для обеспечения защиты систем и данных					

11. Настройка IPSec для сбора событий информационной безопасности	4	4	0	ПК-5.В/НИ.2	Сбор событий информационной безопасности
12. Сбор событий безопасности в подсистеме аудита Linux	4	4	0	ПК-5.В/НИ.2	Сбор событий информационной безопасности
13. Автоматизация сбора событий безопасности	6	6	0	ПК-5.В/НИ.2	Сбор событий информационной безопасности
14. Администрирование систем управления инцидентами информационной безопасности	4	4	0	ПК-5.В/НИ.2	Администрирование систем управления инцидентами информационной безопасности

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Настройка IPSec для сбора событий информационной безопасности	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
2	Сбор событий безопасности в подсистеме аудита Linux	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
3	Автоматизация сбора событий безопасности	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
4	Администрирование систем управления инцидентами информационной безопасности	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: 9				
1	Подготовка к занятиям	ПК-3.В/КА.3,ПК-4.В/ПР.3,ПК-5.В/НИ.2	40	10
: Рудаков А. В. Операционные системы и среды : учебник / А. В. Рудаков. — Москва : КУРС : ИНФРА-М, 2025. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - URL: https://znanium.ru/catalog/product/2184032 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.				
2	Дополнительная учебная деятельность	ПК-3.В/КА.3,ПК-4.В/ПР.3,ПК-5.В/НИ.2	24	0

: Рудаков А. В. Операционные системы и среды : учебник / А. В. Рудаков. — Москва : КУРС : ИНФРА-М, 2025. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - URL: https://znanium.ru/catalog/product/2184032 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.				
3	Подготовка к аттестации	ПК-3.В/КА.3,ПК-4.В/ПР.3,ПК-5.В/НИ.2	40	10
: Рудаков А. В. Операционные системы и среды : учебник / А. В. Рудаков. — Москва : КУРС : ИНФРА-М, 2025. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - URL: https://znanium.ru/catalog/product/2184032 (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		
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
ПК-3.В/КА	ПК-3.В/КА 3. Знает нормативно-методическую базу по осуществлению контрольно-аналитической деятельности		+
ПК-4.В/ПР	ПК-4.В/ПР 3. Знает принципы построения систем защиты информации, включая настройку таких систем и их компонентов		+
ПК-5.В/НИ	ПК-5.В/НИ 2. Умеет производить исследования по оценке защищённости информации от утечек по техническим каналам и осуществлять анализ их результатов		+

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

5. Литература

Основная литература

1. Баланов А. Н. Разработка систем с повышенными требованиями к безопасности : учеб. пособие / А. Н. Баланов. – Москва : Агентство электронных изданий «Интермедиатор», 2026. - 112 с. – (Айтишный университет. Специалист). - ISBN 978-5-91349-141-1. - URL: https://znanium.ru/catalog/product/2265301 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

2. Ларина Т. Б. Администрирование операционных систем. Мониторинг и планирование заданий : учеб. пособие / Т. Б. Ларина. - Москва : РУТ (МИИТ), 2018. - 75 с. - URL: https://znanium.com/catalog/product/1895276 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

Дополнительная литература

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.

2. 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 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

Интернет-ресурсы

1. National vulnerability database. – Text : electronic // NIST : website. – URL: https://nvd.nist.gov/ (access date: 02.07.2026).

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Рудаков А. В. Операционные системы и среды : учебник / А. В. Рудаков. — Москва : КУРС : ИНФРА-М, 2025. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - URL: https://znanium.ru/catalog/product/2184032 (дата обращения 26.06.2026). – Режим доступа: по подписке. - Текст : электронный.

6.2 Специализированное программное обеспечение

1 ПО для виртуализации Vmware, Inc. Vmware

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