

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
"Дальневосточный государственный университет путей сообщения"  
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и  
системы

Попов М.А., канд. техн.  
наук, доцент



11.06.2021

## РАБОЧАЯ ПРОГРАММА

дисциплины **Методы моделирования и исследования угроз информационной безопасности  
автоматизированных систем**

для направления подготовки 09.04.02 Информационные системы и технологии

Составитель(и): к.ф.-м.н, доцент, доцент, Карачанская Е.В.

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 09.06.2021г. № 6

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от  
11.06.2021 г. № 6

---

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2023 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2024 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2025 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

---

---

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК РНС

\_\_ \_\_\_\_\_ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от \_\_ \_\_\_\_\_ 2026 г. № \_\_  
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины Методы моделирования и исследования угроз информационной безопасности автоматизированных систем  
разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 917

Форма обучения **очная**

**ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		зачёты с оценкой 2
контактная работа	54	РГР
самостоятельная работа	90	2 сем. (1)

**Распределение часов дисциплины по семестрам (курсам)**

Семестр (<Курс>.<Семестр на курсе>)	2 (1.2)		Итого	
	уп	рп	уп	рп
Неделя	16			
Вид занятий	уп	рп	уп	рп
Лекции	32	32	32	32
Практические	16	16	16	16
Контроль самостоятельной работы	6	6	6	6
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	54	54	54	54
Сам. работа	90	90	90	90
Итого	144	144	144	144

### 1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Угрозы и их источники безопасности информационно - телекоммуникационным системам. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах. Основные задачи обеспечения безопасности информации в информационных системах. Математические метода моделирования угроз. Методы исследования угроз информационной безопасности автоматизированных систем. Использование инструментальных средств для анализа защищенности объектов информатизации. Требования нормативно-методических документов по защите информации. Классический подход. Официальный подход. Организация контроля эффективности защиты объектов информатизации. Формирование модели угроз информационной системе. Определение актуальности угроз. Математические способы анализа защищенности объектов информатизации и информационных систем. Анализ защищенности информационных систем на основе моделирования угроз. Критерии оценки эффективности. Требования к средствам контроля эффективности защиты информации. Основные подходы к анализу защищенности объектов информатизации средствами контроля.
-----	---

### 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код дисциплины:	Б1.В.02
<b>2.1</b>	<b>Требования к предварительной подготовке обучающегося:</b>
2.1.1	Компьютерные, сетевые и информационные технологии
2.1.2	Планирование научного эксперимента и обработка экспериментальных данных
<b>2.2</b>	<b>Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>
2.2.1	Методы проектирования защищенных информационных систем
2.2.2	Научно-исследовательская работа
2.2.3	Преддипломная практика

### 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

<b>ПК-1: Способен осуществлять сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования</b>	
<b>Знать:</b>	
принципы построения систем защиты информации, критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем, знает основные угрозы безопасности информации и политику безопасности	
<b>Уметь:</b>	
Применять методы сбора и анализ научнотехнической информации, отечественного и зарубежного опыта необходимых для безопасности операционных систем; социальных и образовательных проблем информатики; психологии и педагогике	
<b>Владеть:</b>	
Навыками сбора и анализ научнотехнической информации, отечественного и зарубежного опыта необходимых для безопасности операционных систем; социальных и образовательных проблем информатики; психологии и педагогике	
<b>ПК-4: Способен осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований</b>	
<b>Знать:</b>	
Основы моделирования процессов и объектов, стандартные пакеты автоматизированного проектирования и исследований информационных процессов и технологий	
<b>Уметь:</b>	
Осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований информационных процессов и технологий	
<b>Владеть:</b>	
Навыками моделирования процессов и объектов, стандартные пакеты автоматизированного проектирования информационных процессов и технологий	
<b>ПК-5: Способен осуществлять постановку и проведение экспериментов по заданной методике и анализ результатов</b>	
<b>Знать:</b>	
Основы проведения экспериментов по заданной методике систем обработки информации; экспериментальных данных и анализ результатов	
<b>Уметь:</b>	
Осуществлять постановку и проведение экспериментов по заданной методике систем обработки информации; экспериментальных данных и анализ результатов.	
<b>Владеть:</b>	

Навыками проведения экспериментов по заданной методике систем обработки информации; экспериментальных данных и анализ результатов.

**4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	<b>Раздел 1. содержание курса</b>						
1.1	Угрозы и их источники безопасности информационно - телекоммуникационным системам. /Лек/	2	2	ПК-1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1	0	
1.2	Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах. /Лек/	2	2	ПК-4 ПК-5	Л1.1 Л1.3Л2.2 Э1	0	<a href="https://www.garant.ru/products/ipo/prime/doc/400325044/">https://www.garant.ru/products/ipo/prime/doc/400325044/</a>
1.3	Основные задачи обеспечения безопасности информации в информационных системах. /Лек/	2	2	ПК-4 ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/">https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/</a> <a href="https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/">https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/</a>
1.4	Математические методы моделирования угроз. /Лек/	2	6	ПК-4	Л1.1 Л1.3Л2.2	0	
1.5	Методы исследования угроз информационной безопасности автоматизированных систем. /Лек/	2	2	ПК-4 ПК-1	Л1.1 Л1.3Л2.2	0	<a href="https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/">https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/</a>
1.6	Использование инструментальных средств для анализа защищенности объектов информатизации /Лек/	2	2	ПК-4 ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://www.garant.ru/products/ipo/prime/doc/400325044/">https://www.garant.ru/products/ipo/prime/doc/400325044/</a>
1.7	Требования нормативно-методических документов по защите информации. Классический подход. Официальный подход. Организация контроля эффективности защиты объектов информатизации. /Лек/	2	2	ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://www.garant.ru/products/ipo/prime/doc/400325044/">https://www.garant.ru/products/ipo/prime/doc/400325044/</a>
1.8	Формирование модели угроз информационной системе. Определение актуальности угроз. /Лек/	2	4	ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/">https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/</a>
1.9	Математические способы анализа защищенности объектов информатизации и информационных систем. /Лек/	2	4	ПК-4 ПК-1	Л1.1 Л1.3Л2.2	0	

1.10	Анализ защищенности информационных систем на основе моделирования угроз. Критерии оценки эффективности. /Лек/	2	4	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/">https://sudact.ru/law/metodicheskie-dokumenty-metodika-otsenki-ugroz-bezopasnosti-informatsii/metodika/2/</a>
1.11	Требования к средствам контроля эффективности защиты информации. Основные подходы к анализу защищенности объектов информатизации средствами контроля. /Лек/	2	2	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://www.garant.ru/products/ipo/prime/doc/400325044/">https://www.garant.ru/products/ipo/prime/doc/400325044/</a>
1.12	Общая математическая модель защиты информации /Пр/	2	4	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2	0	<a href="https://cyberleninka.ru/article/n/obschaya-matematicheskaya-model-zaschity-informatsii">https://cyberleninka.ru/article/n/obschaya-matematicheskaya-model-zaschity-informatsii</a>
1.13	Математические модели защиты информации в ИС (модель Лотки-Вольтерры, модель Ланчестера) /Пр/	2	4	ПК-1 ПК-5	Л1.1 Л1.3Л2.2	4	работа со статьями <a href="https://habr.com/ru/company/vps_house/blog/347088/">https://habr.com/ru/company/vps_house/blog/347088/</a> <a href="https://www.hse.ru/data/641/164/1241/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B5%D1%84%D0%B5%D1%80%D0%B0%D1%82_31.11.2004.pdf">https://www.hse.ru/data/641/164/1241/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B5%D1%84%D0%B5%D1%80%D0%B0%D1%82_31.11.2004.pdf</a> <a href="https://cyberpedi.a.su/11x2dd8.html">https://cyberpedi.a.su/11x2dd8.html</a> <a href="https://masters.donntu.org/2013/fknt/shumskiy/library/article8.pdf">https://masters.donntu.org/2013/fknt/shumskiy/library/article8.pdf</a>
1.14	Построение формальной модели защиты ИС (графовая модель угроз, расчет параметров модели /Пр/	2	4	ПК-1 ПК-5	Л1.1 Л1.3Л2.2 Э1	0	<a href="https://books.ifmo.ru/file/pdf/1763.pdf">https://books.ifmo.ru/file/pdf/1763.pdf</a>
1.15	Требования к средствам контроля эффективности защиты информации. Основные подходы к анализу защищенности объектов информатизации средствами контроля. /Пр/	2	4	ПК-1 ПК-5	Л1.1 Л1.3Л2.2	4	работа в малых группах
<b>Раздел 2. Самостоятельная работа</b>							
2.1	выполнение РГР /РГР/	2	30	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2	0	
2.2	подготовка к лекционным и практическим занятиям /Ср/	2	52	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2	0	
2.3	Зачет с оценкой /Ср/	2	8	ПК-4 ПК-1 ПК-5	Л1.1 Л1.3Л2.2 Э1	0	

**5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

Размещены в приложении

**6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)****6.1. Рекомендуемая литература****6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)**

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Березюк Л.П.	Организационное обеспечение информационной безопасности: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,
Л1.2	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций	М. Берлин: Директ-Медиа, 2015, <a href="http://biblioclub.ru/index.php?page=book&amp;id=362895">http://biblioclub.ru/index.php?page=book&amp;id=362895</a>
Л1.3	Нестеров С. А.	Основы информационной безопасности	Санкт-Петербург: Издательство Политехнического университета, 2014, <a href="http://biblioclub.ru/index.php?page=book&amp;id=363040">http://biblioclub.ru/index.php?page=book&amp;id=363040</a>

**6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)**

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Бабаш А. В., Баранова Е. К.	Информационная безопасность. Лабораторный практикум: учеб. пособие	Москва: КноРус, 2016,
Л2.2	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,
Л2.3	В.И. Аверченков	Системы защиты информации в ведущих зарубежных странах	Москва: Флинта, 2011, <a href="http://biblioclub.ru/index.php?page=book&amp;id=93351">http://biblioclub.ru/index.php?page=book&amp;id=93351</a>

**6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

Э1	МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРАКТИКУМ	<a href="https://publications.hse.ru/mirror/pubs/share/folder/w8p5lbfvz1/direct/203455445.pdf">https://publications.hse.ru/mirror/pubs/share/folder/w8p5lbfvz1/direct/203455445.pdf</a>
----	---	---

**6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)****6.3.1 Перечень программного обеспечения**

Visio Pro 2007 - Векторный графический редактор, редактор диаграмм и блок-схем, лиц.45525415
Windows 7 Pro - Операционная система, лиц. 60618367
Антивирус Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition - Антивирусная защита, контракт 469 ДВГУПС
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)

**6.3.2 Перечень информационных справочных систем**

Профессиональная база данных, информационно-справочная система Гарант - <a href="http://www.garant.ru">http://www.garant.ru</a>
Профессиональная база данных, информационно-справочная система КонсультантПлюс - <a href="http://www.consultant.ru">http://www.consultant.ru</a>

**7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Аудитория	Назначение	Оснащение
101/1	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 4Gb, int Video, 1 Tb, DVD+RW, ЖК 19"
101	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 4Gb, int Video, 1 Tb, DVD+RW, ЖК 19"

Аудитория	Назначение	Оснащение
	для самостоятельной работы.	
104/2	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23"
104/1	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23", доска
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя

#### 8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Видами аудиторной работы студента при изучении дисциплины являются лекции и практические занятия. Студент обязан посещать аудиторские занятия. На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать лекционный материал. При необходимости студент имеет право задать вопрос в отношении изложенного материала во время, отведенное для этих целей преподавателем.

По подготовке к лабораторным занятиям

На практических занятиях излагаются и разъясняются основные понятия темы, связанные с выполнением практических заданий, даются рекомендации для самостоятельной работы и выполнения РГР. При подготовке к практическим занятиям студент должен изучить вопросы ранее рассмотренные на лекционных занятиях.

По организации самостоятельной работы

Для студентов самостоятельная работа является одним из основных видов работы по изучению дисциплины. Она включает

- изучение материала установочных занятий;
- работу с рекомендованной литературой и дополнительными источниками информации;
- подготовку к сдаче зачета и экзамена.

Самостоятельную работу по изучению дисциплины целесообразно начинать с изучения рабочей программы, которая содержит основные требования к знаниям, умениям, навыкам обучаемых, ознакомления с разделами и темами.

Для лиц с ограниченными возможностями используются дистанционные образова-тельные технологии, а именно сайт ДВГУПС <http://www.dvgups.ru/> и рабочая программа дисциплины.