

Федеральное государственное бюджетное учреждение науки
Институт машиноведения им. А.А. Благонравова
Российской академии наук
(ИМАШ РАН)

УТВЕРЖДАЮ

Заместитель директора по вопросам
подготовки кадров высшей
квалификации ИМАШ РАН

к.ф-м.н. Жданов Э.Р.

« 01 » 11 2026 года

М.П.



Рабочая программа дисциплины
«Информационная безопасность»

Направление подготовки:	02.04.03 Математическое обеспечение и администрирование информационных систем
Профиль подготовки:	Искусственный интеллект и интеллектуальная обработка данных
Квалификация:	Магистр
Форма обучения	Очная

Москва, 2026 г.

1. Аннотация к дисциплине

1.1.	Составлена в соответствии с ФГОС ВО - магистратура по направлению подготовки 02.04.03 Математическое обеспечение и администрирование информационных систем, утвержденным приказом Минобрнауки от 23.08.2017г. № 812.
1.2.	Закладывает основы для разработки комплекса мер по обеспечению защиты информационных активов организации путем их идентификации, описания, выявления уязвимостей, угроз, а также рисков, которые могут произойти в случае реализации угроз применительно к имеющимся уязвимостям информационных активов. При этом комплекс мер основывается на соответствующей нормативно-правовой базе, включающей как федеральные законы и документы регулирующих государственных органов, так и стандарты, лучшие практики, отраслевые и локальные документы, а также организационном, аппаратном и программном обеспечении.

2. Место дисциплины в структуре ООП

2.1.	Цикл (раздел) ООП: Б1.В.ОД.4
2.2.	2 курс, 3 семестр

3. Цель освоения дисциплин

3.1.	Формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы
------	---

4. Задачи освоения дисциплины

4.1.	- сформировать знания, умения и практический опыт осуществления поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач; - решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - сформировать знания, умения и практический опыт инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем в области защиты информации; - научиться применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой.
------	---

5. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

ПК-2	Управление работами системных аналитиков
ПК-2.1	Разработка методик выполнения работ подчиненными системными аналитиками на всем жизненном цикле
ПК-2.2	Контроль и координация работ, выполняемых подчиненными системными аналитиками

Код индикатора компетенции	Планируемые результаты обучения по дисциплине
ПК-2.1	Знать: - нормативно-правовые акты РФ и международные стандарты в области ИБ. - методологию Secure SDLC и принципы интеграции ИБ в процессы разработки. - специфику угроз ИБ для систем искусственного интеллекта и методы их классификации. Уметь: - формулировать требования к информационной безопасности в составе технических заданий. - разрабатывать регламенты и инструкции для подчиненных аналитиков по выполнению работ с учетом требований ИБ.

	- оценивать риски ИБ на этапах анализа и проектирования системы. <i>Иметь практический опыт:</i> - разработки методики выполнения работ по анализу защищенности системы на этапе сбора требований. - создания регламента для подчиненных по верификации реализации мер защиты в проектной документации.
ПК-2.2	<i>Знать:</i> - методы и инструменты контроля качества выполнения работ с точки зрения информационной безопасности. - принципы координации действий команды при выявлении инцидентов или уязвимостей. - порядок документирования результатов контроля и отчетности перед руководством. <i>Уметь:</i> - осуществлять контроль за соблюдением утвержденных методик и регламентов по ИБ при выполнении работ подчиненными. - координировать действия команды по устранению выявленных уязвимостей в установленные сроки. - проводить аудит промежуточных результатов работы на соответствие требованиям безопасности. <i>Иметь практический опыт:</i> - координации работы группы аналитиков при проведении моделирования угроз для сложной ИИ-системы. - подготовки отчета о результатах контроля выполнения работ с указанием выявленных отклонений от стандартов ИБ.

6. Тематический план

Наименование темы/раздела	Виды занятий и трудоемкость (в часах)					Формы контроля Форма ПА
	Всего	Л	ПЗ	ЛЗ	СР	
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	38	4	6	4	24	Отчет по лабораторному практикуму /20 Реферат/10
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	34	4	-	6	24	Отчет по лабораторному практикуму /20
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	32	2	-	6	24	Отчет по лабораторному практикуму /20
Тема 4. Защита информации в информационных системах	40	2	6	8	24	Отчет по лабораторному практикуму /20 Эссе/10
Всего часов	144	12	12	24	96	100 ТКУ
Контроль, час	36					Экзамен
Объем дисциплины (в ак.ч.)	180					
Объем дисциплины (в з.е.)	5					

7. Содержание дисциплины

Наименование темы/раздела	Краткое содержание	Лекции часов
Тема 1. Общие проблемы	Основные понятия информационной безопасности	4

безопасности. Основные положения теории информационной безопасности	(ИБ). Понятие тайны как объекта защиты ИБ. Организация защиты информации (ЗИ). Политика ИБ. Субъекты и средства, представляющие угрозу для ИБ. Субъекты и средства, осуществляющие защиту информации.	
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	Основы нормативно-правовой ЗИ. Основные нормативные документы РФ по ЗИ. Защита государственной тайны. Защита коммерческой тайны (КТ). Доктрина ИБ РФ. Государственные органы РФ, отвечающие за нормативно-правовое обеспечение ИБ.	4
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Классификация способов защиты информации. Основные действия по защите информации. Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.	2
Тема 4. Защита информации в информационных системах	Основные принципы организации процесса защиты информации. Угрозы информационной безопасности. Средства защиты информации. Защита информации от утечки по техническим каналам. Оценка эффективности системы ИБ. Средства несанкционированного доступа и защиты аудиоинформации. Средства несанкционированного доступа и защиты видеоинформации.	2

8. Самостоятельная работа студентов

Наименование темы/раздела	Виды самостоятельной работы	Трудоемкость в часах
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	Работа с литературой, ЭБС, источниками в сети Internet, подготовка заданий для сдачи текущего контроля успеваемости, подготовка реферата	24
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	Работа с литературой, ЭБС, источниками в сети Internet, подготовка заданий для сдачи текущего контроля успеваемости	24
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	Работа с литературой, ЭБС, источниками в сети Internet, подготовка заданий для сдачи текущего контроля успеваемости	24
Тема 4. Защита информации в информационных системах	Работа с литературой, ЭБС, источниками в сети Internet, подготовка заданий для сдачи текущего контроля успеваемости	24

9. Тематика практических и лабораторных занятий

Наименование темы/раздела	Вид занятия	Краткое содержание занятия	Объем часов
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	лабораторный практикум	Выполнение заданий в лабораторных условиях	4

Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	семинар	Защита рефератов и обсуждение	6
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	лабораторный практикум	Выполнение заданий в лабораторных условиях	6
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	лабораторный практикум	Выполнение заданий в лабораторных условиях	6
Тема 4. Защита информации в информационных системах	лабораторный практикум	Выполнение заданий в лабораторных условиях	8
Тема 4. Защита информации в информационных системах	семинар	Обсуждение проблемных тем и написание эссе	6

10. Фонд оценочных средств

12.1. Контрольные вопросы и задания для проведения текущего контроля
В приложении
12.2. Фонд оценочных средств для проведения промежуточной аттестации
В приложении
12.3. Порядок начисления баллов и критерии оценивания
В приложении

11. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература			
Авторы	Заглавие	Издательство, год	Эл. адрес
Зенков, А. В.	Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп.	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/588741
9.2. Дополнительная литература			
Авторы	Заглавие	Издательство, год	Эл. адрес
Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Организационное и правовое обеспечение информационной безопасности: учебник для вузов	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/583236
Щеглов, А. Ю.	Защита информации: основы теории учебник для вузов	Москва: Издательство Юрайт, 2026	urait.ru/bcode/583858
Щербак, А. В.	Информационная безопасность: учебник для вузов / А. В. Щербак. — 2-е изд.	Москва: Издательство Юрайт, 2026	https://urait.ru/bcode/589902

12. Материально-техническое обеспечение дисциплины

Учебные помещения	кабинеты оснащены мебелью и оборудованием, соответствующими санитарным нормам и требованиям техники безопасности.
Информационно-технологическая инфраструктура	- серверы и хостинг: наличие сервера или облачного хранилища для размещения учебных ресурсов и платформ электронного обучения; - интернет-канал: стабильный широкополосный доступ к интернету

	для бесперебойной передачи больших объемов данных.
<i>Организационное обеспечение</i>	- технические средства обучения: компьютеры, ноутбуки, планшеты и мобильные устройства; - программы для видеоконференцсвязи для проведения лекций, консультаций и практических занятий в режиме реального времени; - антивирусное ПО и защита данных для предотвращения утечек конфиденциальной информации и защиты пользователей от киберугроз.
<i>Условия взаимодействия участников образовательного процесса</i>	- дистанционная поддержка преподавателей: помощь техническими специалистами настройки оборудования и программного обеспечения. - поддержка слушателя: организация технической поддержки, включая инструкции по установке и настройке необходимых приложений, устранение возникающих проблем.