МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет химической технологии и биотехнологии

УТВЕРЖДАЮ
Декан
_____ / А.С. Соколов /
«26» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность автоматизированных систем»

Направление подготовки
15.03.04 Автоматизация технологических процессов и производств

Профиль «Автоматизация технологических производств»

Квалификация
Бакалавр

Форма обучения
Очная

Москва, 2026

Разработчик:

Доцент, к.т.н. доцент кафедры «Аппаратурное оформление и автоматизация технологических производств имени профессора М.Б. Генералова»

/Д.В. Зубов /

Согласовано:

Заведующий кафедрой «Аппаратурное оформление и автоматизация технологических производств имени профессора М.Б. Генералова»,
к.т.н.

/А.С. Кирсанов/

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине

Обучение по дисциплине «Информационная безопасность автоматизированных систем» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1 Способность разрабатывать и применять методы искусственного интеллекта и машинного обучения для решения профессиональных задач	ИПК-1.1. Выбирает методы и инструментальные средства искусственного интеллекта и машинного обучения для решения задач в зависимости от особенностей проблемной и предметной областей; ИПК-1.2. Определяет метрики оценки результатов моделирования и критерии качества построенных моделей; ИПК-1.3. Принимает участие в оценке, выборе и при необходимости разработке методов искусственного интеллекта и машинного обучения.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемая участниками образовательных отношений блока Б1 «Дисциплины (модули)».
Дисциплина непосредственно связана со следующими дисциплинами и практиками ООП: Информационные технологии; Системы реального времени.

3. Структура и содержание дисциплины

3.1 Виды учебной работы и трудоемкость

№ п/п	Вид учебной работы	Количество часов	Семестры
			7
1	**Аудиторные занятия**	**54**	54
	В том числе:		
1.1	Лекции	18	18
1.2	Семинарские/практические занятия	36	36
1.3	Лабораторные занятия		
2	**Самостоятельная работа**	**54**	54
	В том числе:		
2.1	Подготовка к практическим и лабораторным	54	54
3	**Промежуточная аттестация**		
	Зачет/диф.зачет/экзамен		зачёт
	Итого	**108**	108

3.2 Тематический план изучения дисциплины

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Основы информационной безопасности.		2	2			8
2	Модели угроз		2	4			8
3	Симметричное и ассиметричное шифрование		4	4			10
4	Нормативное регулирование информационной безопасности автоматизированных систем		6	12			10
5	Резервное копирование и восстановление		2	4			8
6	Пентест и комплексный анализ защищённости		2	10			10
	Итого	**108**	**18**	**36**			**54**

3.3 Содержание дисциплины

Тема 1. Основы информационной безопасности. Понятия уязвимости, угрозы, атаки.

Понятия идентификации, аутентификации, авторизации. Двухфакторная аутентификация, многофакторная аутентификация.

Тема 2. Модели угроз. Модель STRIDE. Спуфинг(подмена легитимного пользователя), несанкционированное изменение данных, файлов или кода, отказ от авторства, раскрытие информации, отказ в обслуживании, повышение привилегий

Тема 3. Свойство подлинности (Authentication), свойство целостности (Integrity), неотслеживаемость (Non-repudiability). конфиденциальность (Confidentiality). доступность (Availability). принцип авторизации.

Тема 4. Симметричное и ассиметричное шифрование. Алгоритмы ассиметричного шифрования: RSA, DSA, ECC(ECDSA+ ECDH). ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.12-2015, ГОСТ Р 34.10. Электронно-цифровая подпись. Генерация и обмен ключами. TSL, SSH ключи.

Тема 5. Нормативное регулирование информационной безопасности автоматизированных систем: Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 28.08.2024) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации", Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.08.2024) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Тема 6. Пентест. Основные виды пентеста. Инструменты пентеста. Комплексный анализ защищённости. Идентификация и аутентификация (ИАФ). Управление доступом (УПД),

Ограничение программной среды (ОПС). Защита машинных носителей информации (ЗНИ). Аудит безопасности (АУД). Антивирусная защита (АВЗ). Предотвращение вторжений (компьютерных атак) (СОВ). Обеспечение целостности (ОЦЛ). Обеспечение доступности (ОДТ). Защита технических средств и систем (ЗТС). Защита информационной (автоматизированной) системы и ее компонентов (ЗИС). Реагирование на компьютерные инциденты (ИНЦ). Управление конфигурацией (УКФ). Управление обновлениями программного обеспечения (ОПО). Планирование мероприятий по обеспечению безопасности (ПЛН). Обеспечение действий в нештатных ситуациях (ДНС). Информирование и обучение персонала (ИПО)

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1. Семинарские/практические занятия

Семинар 1. Понятия уязвимости, угрозы, атаки.

Семинары 2-3. Модель STRIDE.

Семинар 3. Алгоритмы RSA, DSA, ECC

Семинар 4. Алгоритмы Кузнечик и Магма.

Семинар 5-7. Мероприятия согласно Приказу ФСТЭК России от 25.12.2017 N 239:

Семинар 8-10. Мероприятия согласно Приказу ФСТЭК России 11.02.2013 N 17 (ред. от 28.08.2024).

Семинар 11. Схемы резервного копирования

Семинар 12. Создание образов систем и работа с образами систем.

Семинар 13. Пентест. Основные виды пентеста.

Семинар 14-15. Инструменты пентеста.

Семинар 16-18. Комплексный анализ защищённости.

3.4.2. Лабораторные занятия

Не предусмотрены

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрены

4. Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

ГОСТ Р 34.10. Электронно-цифровая подпись. Генерация и обмен ключами.

Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 28.08.2024) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации",

Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.08.2024) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

4.2 Основная литература

Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 10.01.2026). — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

Назаров, А. Н. Информационная безопасность в сетях общего пользования : учебно-методическое пособие / А. Н. Назаров, Е. Г. Андрианова. — Москва : РТУ МИРЭА, 2023. — 52 с. — ISBN 978-5-7339-1751-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/368963 (дата обращения: 10.01.2026). — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

ЭОР не разработан

4.5 Лицензионное и свободно распространяемое программное обеспечение

Не предусмотрено

4.6 Современные профессиональные базы данных и информационные справочные системы

Интернет-ресурсы включают доступ к электронным библиотекам университета (http://lib.mami.ru/lib/content/elektronyy-katalog), к электронным каталогам вузовских библиотек и крупнейших библиотек Москвы (*http://window.edu.ru*).

5. Материально-техническое обеспечение

Лекции с применением мультимедийного оборудования проводятся в аудиториях кафедры АОиАТП им. проф. М.Б. Генералова. Практические и семинарские занятия проводятся в аудитории 4403 оснащенной необходимым количеством персональных компьютеров для выполнения расчетных работ.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

Основным требованием к преподаванию дисциплины является творческий, проблемно-диалоговый подход, позволяющий повысить интерес студентов к содержанию учебного материала.

Основная форма изучения и закрепления знаний по этой дисциплине – лекционная и практическая. Преподаватель должен последовательно вычитать

студентам ряд лекций, в ходе которых следует сосредоточить внимание на ключевых моментах конкретного теоретического материала, а также организовать проведение практических занятий таким образом, чтобы активизировать мышление студентов, стимулировать самостоятельное извлечение ими необходимой информации из различных источников, сравнительный анализ методов решений, сопоставление полученных результатов, формулировку и аргументацию собственных взглядов на многие спорные проблемы.

Основу учебных занятий по дисциплине составляют лекции. В процессе обучения студентов используются различные виды учебных занятий (аудиторных и внеаудиторных): лекции, семинарские занятия, консультации и т.д. На первом занятии по данной учебной дисциплине необходимо ознакомить студентов с порядком ее изучения, раскрыть место и роль дисциплины в системе наук, ее практическое значение, довести до студентов требования кафедры, ответить на вопросы.

При подготовке к лекционным занятиям по курсу «Информационная безопасность автоматизированных систем» необходимо продумать план его проведения, содержание вступительной, основной и заключительной части лекции, ознакомиться с возможными изменениями в нормативно-технической документации, новинками учебной и методической литературы, публикациями периодической печати по теме лекционного занятия, определить средства материально-технического обеспечения лекционного занятия и порядок их использования в ходе чтения лекции. Уточнить план проведения практического занятия по теме лекции.

В ходе лекционного занятия преподаватель должен назвать тему, учебные вопросы, ознакомить студентов с перечнем основной и дополнительной литературы по теме занятия.

Во вступительной части лекции обосновать место и роль изучаемой темы в учебной дисциплине, раскрыть ее практическое значение. Если читается не первая лекция, то необходимо увязать ее тему с предыдущей, не нарушая логики изложения учебного материала. Лекцию следует начинать, только чётко обозначив её характер, тему и круг тех вопросов, которые в её ходе будут рассмотрены.

В основной части лекции следует раскрывать содержание учебных вопросов, акцентировать внимание студентов на основных категориях, явлениях и процессах, особенностях их протекания. Раскрывать сущность и содержание различных точек зрения и научных подходов к объяснению тех или иных явлений и процессов.

Следует аргументировано обосновать собственную позицию по спорным теоретическим вопросам. Приводить примеры. Задавать по ходу изложения лекционного материала риторические вопросы и самому давать на них ответ. Это способствует активизации мыслительной деятельности студентов, повышению их внимания и интереса к материалу лекции, ее содержанию. Преподаватель должен руководить работой студентов по конспектированию лекционного материала, подчеркивать необходимость отражения в конспектах основных положений изучаемой темы, особо выделяя категорийный аппарат.

В заключительной части лекции необходимо сформулировать общие выводы по теме, раскрывающие содержание всех вопросов, поставленных в лекции. Объявить план очередного семинарского или лабораторного занятия, дать краткие рекомендации по подготовке студентов к семинару или лабораторной работе.

Определить место и время консультации студентам, пожелавшим выступить на семинаре с докладами и рефератами по актуальным вопросам обсуждаемой темы.

Цель практических занятий обеспечить контроль усвоения учебного материала студентами, расширение и углубление знаний, полученных ими на лекциях и в ходе самостоятельной работы. Повышение эффективности практических занятий достигается посредством создания творческой обстановки, располагающей студентов к высказыванию собственных взглядов и суждений по обсуждаемым вопросам, желанию у студентов поработать у доски при решении задач.

После каждого лекционного и практического занятия сделать соответствующую запись в журналах учета посещаемости занятий студентами, выяснить у старост учебных групп причины отсутствия студентов на занятиях. Проводить групповые и индивидуальные консультации студентов по вопросам, возникающим у студентов в ходе их подготовки к текущей и промежуточной аттестации по учебной дисциплине, рекомендовать в помощь учебные и другие материалы, а также справочную литературу.

Изучение дисциплины завершается экзаменом.

Преподаватель, принимающий экзамен, лично несет ответственность за правильность выставления оценки.

6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа является одним из видов получения образования обучающимися и направлена на:

изучение теоретического материала, подготовку к лекционным и семинарским (практическим) занятиям

выполнение контрольных заданий

подготовка к тестированию с использованием общеобразовательного портала.

Самостоятельная работа студентов представляет собой важнейшее звено учебного процесса, без правильной организации которого обучающийся не может быть высококвалифицированным выпускником.

Студент должен помнить, что проводить самостоятельные занятия следует регулярно. Очень важно приложить максимум усилий, воли, чтобы заставить себя работать с полной нагрузкой с первого дня.

Не следует откладывать работу также из-за нерабочего настроения или отсутствия вдохновения. Настроение нужно создавать самому. Понимание

необходимости выполнения работы, знание цели, осмысление перспективы благоприятно влияют на настроение.

Каждый студент должен сам планировать свою самостоятельную работу, исходя из своих возможностей и приоритетов. Это стимулирует выполнение работы, создает более спокойную обстановку, что в итоге положительно сказывается на усвоении материала.

Важно полнее учесть обстоятельства своей работы, уяснить, что является главным на данном этапе, какую последовательность работы выбрать, чтобы выполнить ее лучше и с наименьшими затратами времени и энергии.

Для плодотворной работы немаловажное значение имеет обстановка, организация рабочего места. Нужно добиться, чтобы место работы по возможности было постоянным. Работа на привычном месте делает ее более плодотворной. Продуктивность работы зависит от правильного чередования труда и отдыха. Поэтому каждые час или два следует делать перерыв на 10-15 минут. Выходные дни лучше посвятить активному отдыху, занятиям спортом, прогулками на свежем воздухе и т.д. Даже переключение с одного вида умственной работы на другой может служить активным отдыхом.

Студент должен помнить, что в процессе обучения важнейшую роль играет самостоятельная работа с книгой. Научиться работать с книгой – важнейшая задача студента. Без этого навыка будет чрезвычайно трудно изучать программный материал, и много времени будет потрачено нерационально. Работа с книгой складывается из умения подобрать необходимые книги, разобраться в них, законспектировать, выбрать главное, усвоить и применить на практике.

7. Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю), методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Информационная безопасность автоматизированных систем»

Вид работы	Форма отчетности и текущего контроля
Практические работы	Оформленные отчеты (журнал) практических работ, предусмотренных рабочей программой дисциплины с отметкой преподавателя «удовлетворительно/хорошо/отлично», если выполнены и оформлены все работы.
Лабораторные работы	Оформленные отчеты (журнал) практических работ, предусмотренных рабочей программой дисциплины с отметкой преподавателя «удовлетворительно/хорошо/отлично», если выполнены и оформлены все работы. Правильно выполненные лабораторные работы с соблюдением техники безопасности.

7.2 Шкала и критерии оценивания результатов обучения

7.2.1 Шкала оценивания практической и лабораторной работы

Шкала оценивания	Описание
Неудовлетворительно	Не выполнены требования к написанию и защите практической работы: неправильно оформлена работа, неправильно подсчитаны значения, не сформулирован вывод.
Удовлетворительно	Выполнены не все требования к написанию и защите практической работы: неправильно оформлена работа, неправильно сформулирован вывод, но правильно подсчитаны значения.
Хорошо	Выполнены все требования, но с недочетами: незначительные ошибки в оформлении работы, неточности в формулировке выводов. Правильно подсчитаны значения.
Отлично	Выполнены все требования к написанию и защите практической работы: верно подсчитаны значения, сформулирован вывод, соблюдены требования к оформлению.

7.3 Оценочные средства

7.3.1. Текущий контроль

7.3.1.1 Темы практических работ и лабораторных по дисциплине «Информационная безопасность автоматизированных систем»

Тематика практических работ изложена в пункте 3.4.

7.3.2. Промежуточная аттестация

7.3.2.1. Вопросы к зачёту по дисциплине «Информационная безопасность автоматизированных систем»

1 Понятия уязвимости, угрозы, атаки.
2 Понятия идентификации, аутентификации, авторизации.
3 Двухфакторная аутентификация, многофакторная аутентификация.

4 Модели угроз. Модель STRIDE. Спуфинг(подмена легитимного пользователя), несанкционированное изменение данных, файлов или кода, отказ от авторства, раскрытие информации, отказ в обслуживании, повышение привилегий

5 Свойство подлинности (Authentication), свойство целостности (Integrity), неотслеживаемость (Non-repudiability). конфиденциальность (Confidentiality). доступность (Availability). принцип авторизации.

6 Симметричное и ассиметричное шифрование. Алгоритмы ассиметричного шифрования: RSA, DSA, ECC(ECDSA+ ECDH).

7 ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.12-2015, ГОСТ Р 34.10.

8 Электронно-цифровая подпись.

9 Генерация и обмен ключами.

10 TSL, SSH ключи.

11 Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 28.08.2024) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации",

12 Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.08.2024) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

13 Пентест. Основные виды пентеста.

14 Инструменты пентеста.

15 Комплексный анализ защищённости.

16 Управление доступом

17 Ограничение программной среды

18 Аудит безопасности

19 Антивирусная защита

20 Предотвращение вторжений (компьютерных атак)

21 Обеспечение доступности

22 Защита технических средств и систем

23 Защита информационной (автоматизированной) системы и ее компонентов

24 Реагирование на компьютерные инциденты

25 Управление обновлениями программного обеспечения

26 Планирование мероприятий по обеспечению безопасности