МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая документация

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Технологии разработки программного обеспечения

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 5665
Подписал: заведующий кафедрой Нутович Вероника Евгеньевна
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Дисциплина «Техническая документация» формирует у будущих инженеров-программистов критически важную компетенцию в области IT Law и Compliance Engineering – способность обеспечивать соответствие разрабатываемых программных продуктов нормативно-правовым требованиям Российской Федерации и международным стандартам. В условиях тотального импортозамещения и ужесточения регуляторного контроля со стороны Роскомнадзора и ФСТЭК рынок испытывает острый дефицит специалистов, способных выступать связующим звеном между разработчиками, юристами и надзорными органами. Студенты освоят методологии Privacy Impact Assessment, научатся проводить правовой аудит информационных систем персональных данных, формировать матрицы регуляторного соответствия и разрабатывать пакеты compliance-документации для прохождения внешних проверок. Практическая часть дисциплины построена вокруг сквозного кейса по подготовке полного пакета юридически выверенной документации для модельной транспортной информационной системы, работающей с биометрическими данными и геолокацией. Выпускник получает уникальную специализацию Compliance-аналитика, способного транслировать требования 152-ФЗ и отраслевых приказов Минтранса в конкретные технические ограничения, политики обработки данных и регламенты реагирования на инциденты.

Целью освоения дисциплины является формирование у обучающихся системных знаний и практических умений в области правового обеспечения разработки программного обеспечения, методов аудита соответствия информационных систем нормативным требованиям и разработки технической документации, обеспечивающей легитимность эксплуатации ИТ-продуктов в контуре критической информационной инфраструктуры транспортной отрасли.

Для достижения поставленной цели в рамках дисциплины решается комплекс задач, направленных на формирование у обучающихся способности: проводить правовой аудит информационных систем и оценку влияния на конфиденциальность, формировать матрицы регуляторного соответствия с трассируемостью требований от норм закона до технических контролей, разрабатывать Политики обработки персональных данных и регламенты реагирования на инциденты утечки данных в соответствии с требованиями Роскомнадзора, составлять программы внутреннего аудита информационных систем персональных данных и готовить пакеты документации для прохождения внешних регуляторных проверок, применять

специализированный инструментарий Compliance-аналитика для верификации соответствия реализованных технических решений заявленным юридическим требованиям.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-8 - Способен обеспечивать соответствие программных продуктов нормативно-правовым требованиям в сфере информационных технологий.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- нормативно-правовую базу обработки персональных данных в РФ (152-ФЗ, подзаконные акты, требования ФСТЭК и Роскомнадзора) и базовые принципы международных стандартов (GDPR);
- концепцию Privacy Impact Assessment (PIA) и методологии оценки рисков конфиденциальности при внедрении новых информационных систем;
- классификацию информационных систем персональных данных (ИСПДн) и уровни защищенности в соответствии с отраслевыми приказами регуляторов;
- правовые особенности обработки биометрических данных и геолокации в интеллектуальных транспортных системах (требования КИИ и Минтранса);
- принципы Privacy-by-Design и Privacy-by-Default как обязательные ограничения на этапах проектирования архитектуры программного обеспечения;
- архитектурные паттерны обеспечения конфиденциальности (маскирование, псевдонимизация, токенизация) и модели управления доступом (RBAC, ABAC);
- стандарты проектирования безопасных REST API и спецификацию OpenAPI как инструмент формального описания контрактов;
- методологию Data Flow Diagram (DFD) для аудита потоков персональных данных и концепцию Abuse Cases для моделирования угроз;
- структуру и содержание Политики обработки персональных данных (требования ст. 18.1 152-ФЗ) и регламентов реагирования на инциденты утечки данных;

- методологию разработки программ внутреннего аудита ИСПДн и подготовки пакета документов для регуляторных проверок.

Уметь:

- проводить правовой аудит информационных систем при помощи методологии Privacy Impact Assessment при условии анализа потоков персональных данных в транспортных ИС;

- формировать матрицу регуляторного соответствия при помощи методов трассируемости требований при условии маппинга статей 152-ФЗ и GDPR на технические контролИ;

- разрабатывать Политику обработки персональных данных при помощи шаблонов Роскомнадзора при условии соответствия требованиям ст. 18.1 152-ФЗ;

- составлять регламенты реагирования на инциденты утечки данных при помощи методологии Data Breach Response при условии соблюдения сроков уведомления регулятора;

- разрабатывать программы внутреннего аудита ИСПДн при помощи требований ФСТЭК при условии подготовки системы к внешним регуляторным проверкам;

- составлять аналитические записки о рисках несоответствия при помощи методов risk assessment при условии приоритизации нарушений по тяжести последствий.

Владеть:

- навыками работы со специализированным инструментарием Compliance-аналитика для аудита существующих информационных систем;

- методами автоматизированной верификации трассируемости требований в реляционных базах данных;

- приемами нормоконтроля и структурирования юридических документов в среде отечественных офисных пакетов;

- навыками анализа модельных логов доступа для локализации инцидентов и формирования форензик-отчетов.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 60 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Нормативно-правовой фундамент IT-комплаенса в РФ Рассматриваемые вопросы: - нормативно-правовая база обработки персональных данных в РФ (152-ФЗ, подзаконные акты, требования ФСТЭК и Роскомнадзора); - правовая классификация персональных данных (общие, специальные, биометрические, иные); - базовые принципы международных стандартов (GDPR) и их влияние на экспортные ИТ-продукты.
2	Специфика транспортных ИС и критической информационной инфраструктуры Рассматриваемые вопросы: - правовые основы обработки геолокации и телеметрии в транспортных системах; - требования к критической информационной инфраструктуре (КИИ) в транспортной отрасли; - отраслевые приказы Минтранса и их влияние на архитектуру ИС.
3	Методология Privacy Impact Assessment (PIA) Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- концепция Privacy Impact Assessment (PIA) и этапы проведения оценки; - методология Data Mapping для инвентаризации потоков персональных данных; - моделирование угроз конфиденциальности и концепция Abuse Cases.
4	Оценка рисков и матрица соответствия Рассматриваемые вопросы: - методы оценки рисков (risk assessment) и приоритизация нарушений; - матрица трассируемости требований (RTM) как инструмент аудита; - формирование матрицы регуляторного соответствия.
5	Политика обработки ПДн и уведомления регулятора Рассматриваемые вопросы: - структура и содержание Политики обработки персональных данных (требования ст. 18.1 152-ФЗ); - уведомления Роскомнадзора об обработке персональных данных и изменениях в обработке; - соглашения с обработчиками персональных данных и трансграничная передача данных.
6	Регламенты реагирования на инциденты Рассматриваемые вопросы: - регламенты реагирования на инциденты утечки данных (Data Breach Response); - сроки и порядок уведомления регулятора и субъектов персональных данных; - анализ судебных прецедентов и штрафов за нарушения.
7	Организация внутреннего аудита ИСПДн Рассматриваемые вопросы: - методология разработки программ внутреннего аудита ИСПДн; - составление чек-листов для проверки реализации технических контролей; - документирование результатов аудита и планов устранения нарушений.
8	Подготовка к регуляторным проверкам Рассматриваемые вопросы: - подготовка пакета документов для регуляторных проверок (Роскомнадзор, ФСТЭК); - типовые нарушения и рекомендации по их устранению; - защита compliance-решений перед руководством и аудиторами.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Классификация информационных систем персональных данных Студент анализирует предоставленную бизнес-модель транспортной ИС и идентифицирует категории обрабатываемых персональных данных. На основе требований ФСТЭК и Постановления Правительства РФ обучающийся определяет актуальные угрозы и устанавливает требуемый уровень защищенности системы. Результатом работы является заполненный паспорт ИСПДн с обоснованием класса защищенности.
2	Автоматизация формирования паспорта ИСПДн Студент загружает реестр полей базы данных в специализированный калькулятор на базе электронных таблиц с зашитыми макросами. Обучающийся параметризует формулы в соответствии с критериями Приказа ФСТЭК № 21 для автоматического расчета уровня защищенности ИСПДн. Итогом работы является сгенерированный проектный документ с обоснованием класса системы и перечнем обязательных мер защиты.
3	Оценка влияния на конфиденциальность (PIA) Студент проводит структурированный анализ потоков биометрических и геолокационных данных в модельной ИС. Обучающийся выявляет уязвимости и оценивает потенциальный ущерб для

№ п/п	Наименование лабораторных работ / краткое содержание
	субъектов данных при реализации различных сценариев злоупотребления. Итогом занятия становится аналитический отчет PIA с реестром выявленных рисков и планом их митигации.
4	Моделирование потоков данных и реестра рисков в САПР Студент применяет среду системного моделирования для визуализации маршрутов движения персональных данных между компонентами модельной транспортной ИС. Обучающийся настраивает атрибуты потоков и связывает выявленные узлы передачи с ячейками матрицы рисков в табличном процессоре. Результатом является интерактивная диаграмма и количественная оценка ущерба для приложения к отчету PIA.
5	Матрица регуляторного соответствия и трассируемость Студент декомпозирует статьи 152-ФЗ и отраслевые приказы Минтранса на конкретные технические и организационные контролИ. Обучающийся строит матрицу трассируемости, связывающую нормативные требования с элементами бизнес-процессов. Результатом является таблица маппинга, готовая для передачи разработчикам в качестве жестких ограничений.
6	Аудит трассируемости требований в реляционных СУБД Студент подключается к существующей базе данных через универсальный SQL-клиент и выполняет запросы к системным каталогам для извлечения метаданных о таблицах и связях. Обучающийся сопоставляет фактическую структуру хранения данных с разработанной матрицей соответствия для выявления полей, не имеющих юридического обоснования. Итогом является отчет о расхождениях между заявленными требованиями и реализованной схемой данных.
7	Разработка Политики обработки персональных данных Студент формулирует публичную Политику обработки персональных данных в строгом соответствии с требованиями статьи 18.1 Федерального закона. Обучающийся разрабатывает шаблоны согласий на обработку данных для различных сценариев взаимодействия с пассажирами. Итоговый документ готовится к публикации на официальном портале модельного транспортного предприятия.
8	Нормоконтроль и структурирование юридических документов Студент разворачивает строгие корпоративные шаблоны в среде отечественного офисного пакета для верстки Политики обработки персональных данных. Обучающийся настраивает автоматическую генерацию оглавления, перекрестных ссылок на статьи 152-ФЗ и применяет стили нормоконтроля к таблицам и приложениям. Результатом является документ, прошедший автоматическую проверку на соответствие требованиям ЕСПД и готовый к публикации.
9	Проектирование матрицы доступа и требований к маскированию Студент формирует матрицу ролевого доступа (RBAC) для персонала транспортной компании с учетом принципа минимальных привилегий. Обучающийся определяет перечень полей базы данных, подлежащих обязательному маскированию или псевдонимизации при выгрузке отчетов. Результатом является спецификация требований к подсистеме безопасности для передачи администраторам баз данных.
10	Проверка механизмов маскирования данных в существующей СУБД Студент анализирует существующие представления и функции базы данных для выявления примененных механизмов псевдонимизации персональных данных. Обучающийся выполняет тестовые SELECT-запросы от имени различных ролей для верификации фактического маскирования биометрических и паспортных данных. Результатом является акт проверки соответствия реализованных механизмов требованиям, сформулированным на практическом занятии.
11	Оценка рисков трансграничной передачи данных Студент анализирует маршруты передачи телеметрии и выявляет юрисдикции, через которые осуществляется транзит данных. Обучающийся разрабатывает проекты дополнительных соглашений с иностранными и отечественными облачными провайдерами. Итогом становится пакет юридических и технических ограничений для настройки сетевой инфраструктуры.

№ п/п	Наименование лабораторных работ / краткое содержание
12	Аудит открытых источников на предмет локализации данных Студент использует публичные реестры регуляторов и базы геолокации IP-адресов для проверки фактического местоположения серверов модельных облачных провайдеров. Обучающийся сверяет полученные сетевые координаты с перечнем стран, обеспечивающих адекватную защиту прав субъектов персональных данных. Результатом является акт аудита локализации данных и список провайдеров, требующих замены.
13	Регламент реагирования на инциденты утечки данных Студент проектирует пошаговый алгоритм действий персонала при обнаружении факта несанкционированного доступа к базе данных пассажиров. Обучающийся рассчитывает нормативные сроки уведомления Роскомнадзора и субъектов данных с учетом выходных дней. Результатом является утвержденный внутренний регламент и шаблоны экстренных уведомлений.
14	Анализ модельных логов доступа для локализации инцидента Студент загружает предоставленный дамп логов авторизации в среду анализа данных и применяет фильтры для выявления аномальных сессий и массовых выгрузок информации. Обучающийся формирует хронологию событий и вычисляет объем скомпрометированных записей для заполнения шаблона экстренного уведомления. Итогом является форензик-отчет, служащий фактологической базой для регламента реагирования.
15	Программа внутреннего аудита ИСПДн Студент составляет комплексный чек-лист для проведения плановой внутренней проверки системы на соответствие заявленной Политике. Обучающийся разрабатывает критерии приемки и шкалу оценки зрелости процессов защиты данных. Итоговый документ служит техническим заданием для службы информационной безопасности предприятия.
16	Автоматизация проверки конфигураций скриптами аудита Студент запускает специализированный скрипт аудита, который считывает метаданные настроек операционной системы и базы данных локальной модельной среды. Обучающийся сопоставляет выгруженные параметры с пунктами разработанного на практическом занятии чек-листа и классифицирует выявленные отклонения. Результатом является автоматически сгенерированный протокол расхождений для плана устранения нарушений.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение рекомендованной литературы.
2	Подготовка к лабораторным работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для СПО / В. И. Петренко, И. В.	Лань : электронно-библиотечная система. — URL:

	Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2026. — 108 с. — ISBN 978-5-507-54557-5. — Текст : электронный	https://e.lanbook.com/book/509353 (дата обращения: 19.06.2026)
2	Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2025. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581505 (дата обращения: 19.06.2026)
3	Информационное право : учебник для вузов / под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2020. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный	Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/466887 (дата обращения: 19.06.2026)
4	Дмитрик, Н. А. Правовая информатика : учебник / Н. А. Дмитрик. — Москва : Infotropic Media, 2022. — 172 с. — ISBN 978-5-9998-0399-3. — Текст : электронный	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/388058 (дата обращения: 19.06.2026)
5	Максуров, А. А. Юридическая технология обеспечения безопасности и защиты персональных данных в сети Интернет : монография / А. А. Максуров. — Москва : Проспект, 2025. — 220 с. — ISBN 978-5-392-42697-3. — Текст : электронный	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/504173 (дата обращения: 19.06.2026)

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями). – Текст : электронный // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz (дата обращения: 05.06.2026).

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – Текст : электронный // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 05.06.2026).

ГОСТ 34.602-2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – Текст : электронный // КонсультантПлюс. – URL: https://docs.cntd.ru/document/1200181804 (дата обращения: 05.06.2026).

ГОСТ 19.402-78. Единая система программной документации. Описание программы. Требования к содержанию и оформлению. – Текст : электронный // КонсультантПлюс. – URL: https://docs.cntd.ru/document/1200006924 (дата обращения: 05.06.2026).

General Data Protection Regulation (GDPR) – Общий регламент по защите данных Европейского Союза. – Текст : электронный // GDPR Info. – URL: https://gdpr-info.eu/ (дата обращения: 05.06.2026).

Privacy Impact Assessment (PIA) Methodology – Методология оценки влияния на конфиденциальность. – Текст : электронный // CNIL. – URL: https://www.cnil.fr/en/privacy-impact-assessment-pia (дата обращения: 05.06.2026).

NIST Privacy Framework – Руководство по управлению рисками конфиденциальности. – Текст : электронный // NIST. – URL: https://www.nist.gov/privacy-framework (дата обращения: 05.06.2026).

Роскомнадзор – Официальный портал для операторов персональных данных. – Текст : электронный // Роскомнадзор. – URL: https://rkn.gov.ru/personal-data/ (дата обращения: 05.06.2026).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Операционные системы – Astra Linux Special Edition / ALT Linux / РЕД ОС.

Офисные пакеты – Р7-Офис / МойОфис (для подготовки compliance-документации и нормоконтроля).

Среда разработки и анализа – Anaconda Distribution, Jupyter Notebook, VS Code Community Edition (оффлайн-версии).

Технологический стек анализа данных (Open Source / РФ) – Python 3.10+, Pandas, NumPy, Matplotlib.

СУБД и клиенты – PostgreSQL / Postgres Pro (в реестре ПО РФ), DBeaver / pgAdmin (для чтения метаданных и аудита).

Системы моделирования – Draw.io / PlantUML (для построения диаграмм потоков данных DFD).

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

Для лабораторных занятий – наличие персональных компьютеров вычислительного класса.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

старший преподаватель кафедры
«Цифровые технологии управления
транспортными процессами» А.Ю. Кремнев

Согласовано:

Заведующий кафедрой ЦТУТП В.Е. Нутович

Председатель учебно-методической
комиссии Н.А. Андриянова