МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ
Проректор по УР О.И. Варфоломеева

Подписано в СДОУ ELMA
Варфоломеева О. И.
06.10.2026 15:56:03

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

(72 часов)
№ 232

Ижевск 2026

Глазовский инженерно-экономический институт

Полное наименование структурного подразделения, представляющего образовательную программу

СОСТАВИТЕЛИ ПРОГРАММЫ:

Пронина И.В., канд. экон. наук, доцент (разделы 1, 3)

Горбушин А.Г., канд.пед.наук, доцент (разделы 2, 4)

Образовательная программа рассмотрена и утверждена на заседании кафедры
Протокол от _____ 20__ г. № _____

Образовательная программа разработана в соответствии

Профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н;

ФГОС ВО по направлению 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021);

ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. N 1553 (ред. от 03.07.2024).

Указать полное наименование документа

Заведующий кафедрой Подписано в СДОУ ELMA Горбушин А. Г. 2026-09-30 11:30:38 А.Г. Горбушин

СОГЛАСОВАНО

Директор ИОТ _____ М.А. Тарасова

Подпись *(Расшифровка подписи)*

Специалист по ОМР 1 категории ИОТ _____ Р.А. Верняева

Подпись *(Расшифровка подписи)*

Разработчики программы:

И.В. Пронина

Подпись *(Расшифровка подписи)*

А.Г. Горбушин

Подпись *(Расшифровка подписи)*

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Глазовский инженерно-экономический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Ижевский государственный технический университет имени М.Т. Калашникова»
(ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ

и.о. проректора по учебной работе

_____ О.И. Варфоломеева

«___»_____2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Глазов 2026

Глазовский инженерно-экономический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Ижевский государственный технический университет имени М.Т. Калашникова»

Составители программы:
Пронина И.В., канд. экон. наук, доцент
Горбушин А.Г., канд.пед.наук, доцент

Образовательная программа рассмотрена и утверждена на заседании кафедры «Машиностроение и информационные технологии»

Протокол от 22.05.2026 №5

Образовательная программа разработана на основании:
Профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н;
ФГОС ВО по направлению 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021);
ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. N 1553 (ред. от 03.07.2024).

Заведующий кафедрой _____ А.Г. Горбушин

СОГЛАСОВАНО

Директор ИОТ _____ М.А. Тарасова

Начальник ОАиМР _____ Е.А. Жданова

Разработчики программы _____ И.В. Пронина
А.Г. Горбушин

Глазовский инженерно-экономический институт (филиал)
федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

УЧЕБНЫЙ ПЛАН
программы повышения квалификации
«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Категория слушателей: лица, имеющие высшее или среднее профессиональное образование
Срок обучения: 72 часа
Форма обучения: очно-заочная

№ п/п	Наименование разделов, тем	Общая трудо-емкость, часов	Всего контактных часов		Контактные часы			СРС, часов	Форма контроля
			синхрон.	асинхрон.	лекции	лабораторные работы	практические и семинарские занятия		
1	**Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных**	**71**	**23**	**10**	**20**		**13**	**38**	
2	**Итоговая аттестация**	**1**	**1**				**1**		**Зачет**
	Итого:	**72**	**24**	**10**	**20**		**14**	**38**	

Глазовский инженерно-экономический институт (филиал)
федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
программы повышения квалификации
«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

№ п/п	Наименование разделов, тем	Общая трудо-емкость, часов	Всего контактных часов		Контактные часы			СРС, часов	Форма контроля
			синхрон.	асинхрон.	лекции	лабораторные работы	практические и семинарские занятия		
1.	**Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных**	**71**	**23**	**10**	**20**		**13**	**38**	
1.1	Правовое, нормативное и методическое обеспечение безопасности персональных данных	14	4	2	4		2	8	Практическое задание
1.2	Угрозы безопасности информационных систем персональных данных	14	4	2	4		2	8	Практическое задание
1.3	Организация обработки персональных данных	14	4	2	4		2	8	Практическое задание
1.4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в ИСПДн	16	6	2	4		4	8	Практическое задание
1.5	Методы защиты информационных систем персональных данных	13	5	2	4		3	6	Практическое задание
2.	**Итоговая аттестация**	**1**	**1**				**1**		**Зачет**
	Итого:	**72**	**24**	**10**	**20**		**14**	**38**	

Календарный учебный график
программы повышения квалификации
«Обеспечение безопасности персональных данных при их обработке
в информационных системах персональных данных»

Неделя	Лекции	Лабораторные работы	Практические и семинарские занятия	Самостоятельная работа	Текущая аттестация	Итоговая аттестация
1 неделя обучения	Тема 1.1 (4 часа)		Тема 1.1 (2 часа)	Тема 1.1 (8 часов)	Практическое задание	
2 неделя обучения	Тема 1.2 (4 часа)		Тема 1.2 (2 часа)	Тема 1.2 (8 часов)	Практическое задание	
3 неделя обучения	Тема 1.3 (4 часа)		Тема 1.3 (2 часа)	Тема 1.3 (8 часов)	Практическое задание	
4 неделя обучения	Тема 1.4 (4 часа)		Тема 1.4 (4 часа)	Тема 1.4 (8 часов)	Практическое задание	
5 неделя обучения	Тема 1.5 (4 часа)		Тема 1.5 (3 часа)	Тема 1.5 (6 часов)	Практическое задание	Зачет (1 час)

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Описание образовательной программы

Программа повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» разработана в соответствии с требованиями Федерального Закона от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации», Приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Программа направлена на формирование у слушателей компетенций, необходимых для организации и реализации мер защиты персональных данных (ПДн) в информационных системах (ИСПДн) различных уровней сложности.

Программа предназначена для специалистов по защите информации, администраторов информационных систем, системных администраторов, юрисконсультов, сотрудников отделов кадров и руководителей подразделений, выступающих в роли операторов ПДн, а также лиц, ответственных за организацию обработки персональных данных в организациях.

Программа разработана в соответствии с:

Профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н;

ФГОС ВО по направлению 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021);

ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 09.12.2016 г. N 1553 (ред. от 03.07.2024).

1.2 Цель образовательной программы

Цель реализации программы: совершенствование и (или) получение новых компетенций, специалистов, работающих в области организации и проведения работ по обеспечению безопасности персональных данных при

их обработке в информационных системах персональных данных (далее – обучающиеся).

Компетенции (трудовые функции) в соответствии с профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах»:

- A/01.5 Проведение технического обслуживания систем защиты информации автоматизированных систем.
- B/01.6 Диагностика систем защиты информации автоматизированных систем.
- B/10.6 Внедрение организационных мер по защите информации в автоматизированных системах.

1.3 Планируемые результаты обучения

Программа направлена на достижение слушателем следующих результатов обучения:

Трудовая функция A/01.5 - Проведение технического обслуживания систем защиты информации автоматизированных систем

Слушатель должен знать:

- законодательные и нормативные правовые акты Российской Федерации в области защиты информации;
- нормативные документы ФСТЭК России и ФСБ России, регламентирующие защиту информации в автоматизированных системах;
- типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях
- классификацию и назначение программных и аппаратных средств защиты информации;
- регламенты, инструкции и методики проведения технического обслуживания СЗИ АС;
- методы контроля работоспособности компонентов СЗИ;
- порядок установки обновлений программного обеспечения СЗИ;
- порядок ведения эксплуатационной и технической документации;
- требования охраны труда при работе со средствами вычислительной техники.

Слушатель должен уметь:

- проводить регламентные работы по техническому обслуживанию СЗИ АС;
- устанавливать обновления и настраивать программные и аппаратные средства защиты информации;
- конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией;
- контролировать работоспособность компонентов СЗИ;
- выявлять и устранять простые неисправности в работе СЗИ;
- вести эксплуатационную и техническую документацию по техническому обслуживанию СЗИ;

- соблюдать требования по защите информации при проведении технического обслуживания.

Трудовая функция B/01.6 — Диагностика систем защиты информации автоматизированных систем

Слушатель должен знать:

- методы и средства диагностики СЗИ АС;
- нормативные правовые акты в области защиты информации;
- признаки и причины возникновения неисправностей и сбоев в работе СЗИ;
- методики анализа защищенности информации в АС;
- специализированное программное обеспечение для диагностики и мониторинга СЗИ;
- порядок проведения контрольных проверок и испытаний СЗИ;
- методы анализа событий информационной безопасности;
- порядок документирования результатов диагностики;
- требования нормативных документов к оценке эффективности СЗИ.

Слушатель должен уметь:

- проводить диагностику и мониторинг состояния СЗИ АС;
- определять источники и причины возникновения инцидентов;
- анализировать события информационной безопасности с использованием специализированных средств;
- выявлять уязвимости и причины нарушения работы СЗИ;
- применять средства диагностики для оценки эффективности СЗИ;
- документировать результаты диагностики и формировать отчетную документацию;
- интерпретировать результаты диагностики и вырабатывать рекомендации по устранению выявленных недостатков.

Трудовая функция B/10.6 - Внедрение организационных мер по защите информации в автоматизированных системах

Слушатель должен знать:

- принципы построения комплексных систем защиты информации;
- нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
- организационные меры и нормативные правовые акты в области защиты информации;
- методы управления инцидентами информационной безопасности;
- подходы к разработке и внедрению политик безопасности в АС;
- требования по защите информации, установленные регуляторами (ФСТЭК России, ФСБ России, Банк России);
- основы менеджмента информационной безопасности (ISO/IEC 27001);
- порядок разработки организационно-распорядительных документов по защите информации;

- методы обучения и информирования пользователей по вопросам защиты информации.

Слушатель должен уметь:

- разрабатывать и корректировать организационные документы по защите информации (политики, регламенты, инструкции);
- реализовывать правила разграничения доступа персонала к объектам доступа;
- внедрять организационные меры в деятельность подразделений;
- проводить обучение пользователей по вопросам защиты информации;
- контролировать соблюдение установленных мер по защите информации;
- организовывать работу по реагированию на инциденты информационной безопасности;
- проводить оценку эффективности внедренных организационных мер.

1.4 Категория слушателей: слушатели, имеющие среднее профессиональное или высшее образование.

1.5 Трудоемкость обучения: 72 академических часа.

1.6 Форма обучения: очно-заочная.

1.7 Применение ЭО и ДОТ: да (синхронные вебинары, доступ к электронным образовательным ресурсам).

2 РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Тема 1. Правовое, нормативное и методическое обеспечение безопасности персональных данных (14 часов)

Вопросы, раскрывающие содержание темы:

Основные понятия, термины и определения в области обеспечения безопасности персональных данных. Персональные данные в Федеральном законе от 27.07.2006 № 152-ФЗ и Трудовом кодексе Российской Федерации. Базовые определения: персональные данные, оператор, обработка ПДн, автоматизированная и неавтоматизированная обработка, информационная система персональных данных (ИСПДн), трансграничная передача, обезличивание ПДн. Соотношение понятий в 152-ФЗ и ТК РФ (гл. 14 «Защита персональных данных работника»). Принципы обработки ПДн (законность, ограничение целей, достоверность, конфиденциальность).

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. Взаимосвязь 152-ФЗ и 149-ФЗ. Категории персональных данных: общедоступные, специальные (раса,

национальность, политические взгляды, религиозные убеждения, состояние здоровья, интимная жизнь), биометрические (физиологические и биологические особенности), иные. Права субъекта персональных данных: право на доступ, уточнение, блокирование, уничтожение ПДн, отзыв согласия на обработку. Обязанности оператора по предоставлению информации субъекту.

Техническая защита информации ограниченного доступа и безопасность персональных данных. Понятие «информация ограниченного доступа» (ст. 2 149-ФЗ). Использование средств криптографической защиты информации (СКЗИ): цели (шифрование, электронная подпись, аутентификация), классификация СКЗИ (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012). Сертифицированные СКЗИ (КриптоПро, VipNet). Лицензирование деятельности по разработке и внедрению СКЗИ. Требования к использованию СКЗИ в ИСПДн для разных уровней защищенности.

Тема 1.2 Угрозы безопасности информационных систем персональных данных (14 часов)

Вопросы, раскрывающие содержание темы:

Общие положения и классификация угроз безопасности персональных данных. Понятие угрозы безопасности ПДн. Общая характеристика уязвимостей ИСПДн: аппаратные, программные, структурно-функциональные, организационные. Классификация угроз по источнику (внешние/внутренние), по характеру воздействия (преднамеренные/непреднамеренные), по целям (нарушение конфиденциальности, целостности, доступности - триада CIA). Банк данных угроз (БДУ) ФСТЭК (УБИ.ХХХ). Методика оценки угроз безопасности информации (утверждена ФСТЭК 05.02.2021) - сценарный подход вместо формул Y1×Y2 (методика 2008) .

Наиболее часто реализуемые угрозы. Угрозы утечки информации по техническим каналам: акустические каналы, электромагнитные излучения (побочные электромагнитные излучения и наводки - ПЭМИН), визуально-оптические каналы. Перехват данных по сетям связи. Угрозы, связанные с хищением носителей (бумажных, электронных). Статистика наиболее распространенных инцидентов утечки ПДн в РФ (2024-2026 гг.).

Угрозы несанкционированного доступа к информации. Угрозы НСД: внутренние и внешние нарушители, их классификация по уровню полномочий и потенциалу. Угрозы программно-математических воздействий: внедрение вредоносного ПО, эксплуатация уязвимостей, использование недекларированных возможностей (НДВ) в системном и прикладном ПО. Угрозы нетрадиционных информационных каналов: социальная инженерия, фишинг, компрометация учетных записей.

Тема 1.3 Организация обработки персональных данных (14 часов)

Вопросы, раскрывающие содержание темы:

Общий порядок организации обработки персональных данных. Порядок уведомления Роскомнадзора об обработке (о намерении осуществлять обработку) персональных данных (ст. 22 152-ФЗ). Исключения из обязанности уведомления. Способы подачи уведомления: в электронном

виде через ЕСИА (Госуслуги), с использованием ЭЦП, на бумажном носителе в территориальный орган Роскомнадзора. Перечень сведений, указываемых в уведомлении: регистрационные реквизиты, цели обработки, категории ПДн, категории субъектов, правовые основания, меры защиты, сроки хранения, третьи лица . Изменения в уведомлении при изменении сведений.

Разработка документации по обработке персональных данных. Состав обязательных документов согласно ст. 18.1 152-ФЗ:

- Приказ о назначении лица, ответственного за организацию обработки ПДн.
- Должностные инструкции для лиц, осуществляющих обработку.
- Политика обработки персональных данных (опубликование или обеспечение неограниченного доступа).
- Перечень мер, необходимых для обеспечения выполнения обязанностей оператора (по Приказу ФСТЭК № 21 / новому проекту).
- Инструкции пользователей ИСПДн.
- Положение о внутреннем контроле.
- Модель угроз (до отмены требования - обязательно; далее - по решению оператора, но определение актуальных угроз обязательно) .

Тема 1.4 Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в ИСПДн (16 часов)

Вопросы, раскрывающие содержание темы:

Общий порядок организации обеспечения безопасности ПДн в ИСПДн. Определение уровня защищенности персональных данных (УЗ-1, УЗ-2, УЗ-3, УЗ-4) на основании категории ПДн, объема данных, типа угроз согласно Постановлению Правительства РФ № 1119. Акт оценки вреда субъектам персональных данных: понятие, виды вреда (материальный, моральный), методика оценки . *Важно:* в 2026 году действующий Приказ ФСТЭК № 21 планируется к отмене с 01.09.2026. Проект нового приказа вводит риск-ориентированный подход и показатель «уровень зрелости».

Состав и содержание мер по обеспечению безопасности ПДн. Состав и содержание мер по обеспечению безопасности ПДн согласно Приказу ФСТЭК № 21 (до 01.09.2026) и проекту нового приказа. Особенности использования средств криптографической защиты информации (СКЗИ) в рамках построения системы защиты персональных данных (СЗПД) в организации. Классификация ИСПДн. Подсистемы криптографической защиты информации в составе СЗПД. Функции подсистемы криптографической защиты информации: шифрование каналов, защита дисковых накопителей, электронная подпись, аутентификация.

Оценка обстановки и формирование замысла защиты персональных данных. Основные этапы при построении системы защиты персональных данных (СЗПД): обследование, классификация, разработка модели угроз, выбор мер, внедрение, аттестация, эксплуатация, мониторинг. Комплекс организационных и технических мероприятий в рамках СЗПД. Новые требования проекта приказа ФСТЭК 2026 года: защита ИИ, интернета вещей

(IoT), облачных вычислений, виртуализации, контейнерных сред, API-интерфейсов, мобильных устройств и удаленного доступа.

Тема 1.5 Методы защиты информационных систем персональных данных (13 часов)

Вопросы, раскрывающие содержание темы:

Особенности обработки персональных данных без использования средств автоматизации. Обработка ПДн на бумажных носителях (Постановление Правительства РФ № 687). Особенности: требование отдельного хранения, ограничение доступа, маркировка, учет носителей, уничтожение. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных (биометрические карты, чипы, иные носители). Правила уничтожения бумажных носителей (шредер, сжигание, пульпа).

Основные обязанности операторов информационных систем, обрабатывающих персональные данные. Ст. 18.1 152-ФЗ: перечень мер, принимаемых оператором. Назначение ответственного за организацию обработки ПДн. Издание локальных актов. Применение правовых, организационных и технических мер. Внутренний контроль соответствия. Оценка вреда субъектам ПДн. Обучение сотрудников. Уведомление Роскомнадзора об инцидентах (в течение 24 часов) и субъектов (в течение 72 часов).

Основные изменения в законе 152-ФЗ «О персональных данных» в 2026 году:

1. Федеральный закон от 26.07.2026 № 265-ФЗ «О внесении изменений в статью 12 Федерального закона «О персональных данных» и отдельные законодательные акты Российской Федерации»:

- Изменения в части 2 статьи 12: уточнен перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн (соответствие Конвенции Совета Европы).
- Внесены изменения в пункт 2 части 5, части 10 и 11 статьи 12 — упрощен порядок трансграничной передачи в государства-участники Конвенции Совета Европы.
- Вступление в силу: со дня официального опубликования (26.07.2026), за исключением ст. 2 (вступает в силу с 01.09.2027).

2. Реформа регуляторных требований ФСТЭК (проект приказа вместо № 21):

- Отмена Приказа ФСТЭК № 21 от 18.02.2013 с 01.09.2026.
- Уход от фиксированного перечня мер (таблицы УЗ-1 — УЗ-4) к риск-ориентированному подходу.
- Введение показателя «уровень зрелости защиты информации» (УЗИ): оценка до начала обработки, затем не реже 1 раза в 3 года, а также после каждого инцидента.
- Два перечня вместо одного: 21 организационное мероприятие и 17 групп технических мер (без жесткой привязки к уровню).
- Новые направления защиты: ИИ, IoT, облака, виртуализация, контейнеры, API, мобильные устройства, веб-технологии.

- Требование взаимодействия с ГосСОПКА для всех операторов ПДн (ранее — только для КИИ).
- Сквозной контроль подрядчиков: оценка уровня зрелости обработчика до заключения договора.
- Модель угроз: разработка перестает быть обязательной (по решению оператора), но определение актуальных угроз остается обязательным.

3. Иные изменения:

- Ужесточение административной ответственности за утечки ПДн (повышенные штрафы по КоАП РФ).
- Новые требования к согласиям на обработку ПДн (формы согласий, запрет на «общие» согласия).
- Обязательность размещения Политики обработки ПДн на сайте организации в случаях, установленных законом.

Перечень практических занятий

Номер темы/ раздела	Наименование практического занятия
1.1	**Анализ нормативной базы и определение статуса оператора** Работа с текстами 152-ФЗ (актуальная редакция 2026 г., с учетом ФЗ № 265-ФЗ), ТК РФ (гл. 14), 149-ФЗ. Анализ кейса: организация обрабатывает ФИО, паспортные данные, СНИЛС, биометрию (отпечатки пальцев для пропускной системы), данные о состоянии здоровья сотрудников. Задача: определить категории ПДн, основания обработки, перечень обязанностей оператора по ст. 18.1, необходимость уведомления Роскомнадзора с учетом исключений (0,5 часа). **Разработка уведомления об обработке ПДн в Роскомнадзор** Изучение требований ст. 22 152-ФЗ и формы уведомления (Приказ Роскомнадзора № 996). Заполнение уведомления на примере организации из кейса. Выбор способа подачи (через ЕСИА, с ЭЦП, на бумажном носителе). Составление проекта уведомления Роскомнадзора об обработке ПДн Анализ изменений в уведомлении при изменении сведений об обработке (1,5 часа)
1.2	**Разработка частной модели угроз с использованием БДУ ФСТЭК** На основе Методики оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021) и Банка данных угроз (БДУ ФСТЭК) для предложенного кейса (розничная сеть с онлайн-кассами и CRM) составить перечень актуальных угроз (не менее 10). Определить источники угроз (внешние/внутренние), возможный ущерб (триада CIA), обосновать актуальность каждой угрозы для данного кейса. Заполнить форму оценки угроз (0,5 часа). **Классификация угроз по техническим каналам и НСД** На основе Методики ФСТЭК для предложенного кейса (типовая

	организация - торговое предприятие) составить перечень актуальных угроз и оценить возможный вред субъектам Разбор конкретных сценариев: 1) Утечка по акустическому каналу (разговор у открытого окна); 2) Перехват ПЭМИН от монитора; 3) Взлом рабочей станции через фишинговое письмо; 4) Инсайдер - увольняющийся сотрудник копирует базу на флешку. Для каждого сценария определить тип угрозы, возможные последствия и предложить превентивные меры (1,5 часа)
1.3	**Разработка проекта Политики обработки персональных данных** На основе ст. 18.1 152-ФЗ разработать проект ПОПДн для условной организации. Отразить: цели и правовые основания, перечень обрабатываемых ПДн, права субъектов, сроки хранения, порядок уничтожения, перечень мер защиты (общие положения). Обсуждение структуры и обязательных разделов (0,5 часа). **Разработка Перечня мер и Инструкции пользователя ИСПДн** Разработка Перечня мер по обеспечению безопасности ПДн с учетом Приказа ФСТЭК № 21 (до 01.09.2026) и проекта нового приказа. Разработка Инструкции пользователя ИСПДн — правила работы с системой, содержащей ПДн, для рядовых сотрудников (понятным языком, с запретами и алгоритмами действий). Разработка проекта «Политики обработки персональных данных» (ст. 18.1 152-ФЗ). Составление «Перечня мер, необходимых для обеспечения выполнения обязанностей оператора» на основании Приказа ФСТЭК № 21. Работа с шаблонами документов (1,5 часа)
1.4	**Определение уровня защищенности ИСПДн и оценка вреда субъектам** Классификация ИСПДн по Постановлению № 1119 и Приказу ФСТЭК № 21. Определение уровня защищенности (УЗ-1 - УЗ-4) для трех разных кейсов: 1) Медицинская клиника (специальные ПДн, 50 000 пациентов); 2) Интернет-магазин (иные ПДн, 100 000 клиентов); 3) Кадровое агентство (иные ПДн, 500 соискателей). Проведение оценки возможного вреда субъектам ПДн по методике Роскомнадзора. Сравнение подходов - УЗ по старой системе и «уровень зрелости» (УЗИ) по проекту нового приказа (1 час). **Проектирование системы защиты ПДн с учетом риск-ориентированного подхода** Изучите Приказ ФСБ № 378 «Об утверждении требований к средствам криптографической защиты...». Составьте перечень ситуаций, когда применение СКЗИ является обязательным. На основании проекта нового приказа ФСТЭК (вместо № 21) разработать концепцию системы защиты ПДн для условной

	организации (дилерский центр, 3 офиса, 200 сотрудников). Определить требуемый «уровень зрелости защиты информации» (УЗИ). Выбрать организационные меры и технические меры. Обосновать выбор. Нарисовать схему защищенной архитектуры (текстовое описание + блок-схема) (3,0 часа)
1.5	**Обработка ПДн без автоматизации и уничтожение носителей** Изучение Постановления № 687 «Об особенностях обработки ПДн без использования средств автоматизации». Практика: разработать регламент уничтожения бумажных носителей (акты, комиссия, способы — шредер, сжигание, пульпа). Разобрать кейс: как уничтожить жесткий диск с ПДн (физическое разрушение, перезапись, дегауссинг). Составить образец Акта об уничтожении (1 час). **Моделирование инцидента и реагирование с учетом новых требований 2026 года** Разработайте план проведения плановой проверки системы защиты ПДн в организации на следующий год. Укажите состав комиссии, перечень проверяемых компонентов, сроки. Составление алгоритма действий при утечке. На основе методических рекомендаций Роскомнадзора составьте пошаговую инструкцию (блок-схему) для ответственного за ПДн при обнаружении факта утечки (от локализации до уведомления субъектов). Кейс: обнаружена утечка ПДн клиентов (25 000 записей) на теневом сайте через уязвимость в необновленном ПО. Задача: 1) Сформировать экстренный штаб; 2) Составить пошаговый план действий по часам (первые 72 часа); 3) Заполнить уведомление в Роскомнадзор (24 часа); 4) Разработать уведомление субъектам (72 часа); 5) Учесть новые требования: уведомление ГосСОПКА, сквозной контроль подрядчиков, оценка уровня зрелости; 6) Составить итоговый акт расследования с корректирующими мерами (2 часа)

Самостоятельная работа

Номер темы/ раздела	Содержание самостоятельной работы
1.1	**Аналитический обзор изменений в законодательстве 2026 года.** Используя официальные сайты Роскомнадзора, ФСТЭК, портал regulation.gov.ru и справочные системы (КонсультантПлюс), найти и изучить следующие документы: 1) Федеральный закон от 26.07.2026 № 265-ФЗ (изменения в ст. 12 152-ФЗ о трансграничной передаче); 2) Проект нового приказа

	ФСТЭК (взамен Приказа № 21) - актуальная редакция на 2026 год; 3) Методику оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021). Составить краткий отчет (2-3 стр.) об основных новациях каждого документа и их влиянии на деятельность оператора ПДн (4 часа). **Определение статуса оператора и границ ИСПДн в своей организации.** Провести анализ: какие ИСПДн используются в вашей организации (или в организации из кейса), какие категории ПДн обрабатываются, какие процессы автоматизированы, а какие ведутся на бумаге. Определить, является ли организация оператором ПДн, требуется ли уведомление Роскомнадзора (с учетом исключений). Составить перечень «пробелов» в текущей системе защиты (что уже есть, чего не хватает). Результат оформить в виде таблицы (4 часа)
1.2	**Построение карты угроз для типового компонента ИСПДн.** Выберите один из компонентов ИСПДн: 1) Веб-сервер (Apache/Nginx) с базой данных клиентов; 2) Рабочая станция сотрудника отдела кадров; 3) Мобильное приложение для клиентов; 4) Сервер баз данных (СУБД) с ПДн. Используя Банк данных угроз (БДУ ФСТЭК) и открытые базы уязвимостей (CVE, SecurityLab), составьте карту угроз (не менее 12 угроз) для выбранного компонента. Для каждой угрозы укажите: номер из БДУ, тип источника (внешний/внутренний), возможный ущерб (C/I/A), обоснование актуальности для типовой российской организации (4 часа). **Анализ реального инцидента утечки ПДн (2024-2026 гг.).** Найдите в открытых источниках (Хабр, SecurityLab, CNews, официальные отчеты Роскомнадзора) описание реальной утечки ПДн (не старше 1 года). Проведите анализ по шаблону: 1) Краткое описание инцидента (кто, когда, сколько записей); 2) Вектор атаки (как злоумышленники проникли); 3) Тип утекших ПДн и объем; 4) Какие меры защиты не были реализованы (или были реализованы некачественно); 5) Последствия для компании (штрафы, суды, репутационные потери). Сделайте вывод: что нужно было сделать, чтобы предотвратить утечку (4 часа)
1.3	**Разработка проекта Политики обработки персональных данных.** На основе требований ст. 18.1 152-ФЗ разработать проект Политики обработки ПДн для организации из кейса (или своей организации). Документ должен содержать: цели и правовые основания обработки (со ссылками на конкретные статьи 152-ФЗ и иных законов), перечень обрабатываемых ПДн по категориям субъектов, права субъектов, условия обработки (согласие, договор, закон), сроки хранения, порядок уничтожения, перечень мер защиты (общие положения). Объем — не менее 10 страниц (с учетом всех обязательных разделов) (4 часа).

	Разработка Перечня мер по обеспечению безопасности ПДн. На основании актуальных требований (Приказ ФСТЭК № 21 до 01.09.2026 и проект нового приказа) разработать Перечень мер для организации. Разделить меры на организационные и технические. Для каждой меры указать: нормативное основание (конкретный пункт приказа), способ реализации, ответственное лицо (должность), срок внедрения. Оформить в виде таблицы (4 часа)
1.4	**Сравнительный анализ сертифицированных СЗИ и СКЗИ.** Изучите реестр сертифицированных средств защиты на сайте ФСТЭК. Выберите одну из категорий: СЗИ от НСД (Secret Net, Dallas Lock, VIPNet, InfoWatch) или СКЗИ (КриптоПро, VipNet CSP, Signal-COM). Проведите сравнительный анализ 3-4 продуктов в выбранной категории по критериям: наличие действующего сертификата ФСТЭК/ФСБ (срок действия), поддерживаемые ОС, функциональные возможности, сложность внедрения (низкая/средняя/высокая), примерная стоимость (укажите порядок цен). Составьте таблицу и напишите краткий вывод о рекомендованном продукте для типовой организации (средний бизнес, 100-500 сотрудников) (5 часов). **Проектирование системы защиты ПДн с учетом риск-ориентированного подхода.** На основе проекта нового приказа ФСТЭК (вместо № 21) разработайте концептуальную схему защиты ПДн для организации (можно использовать диаграмму в Visio или текстовое описание с блок-схемой). Опишите: 1) как определяется уровень зрелости защиты информации (УЗИ) для данной организации; 2) какие организационные мероприятия (из 21-го) выбраны и почему; 3) какие технические меры (из 17 групп) применяются и где именно; 4) как организован сквозной контроль подрядчиков; 5) как обеспечено взаимодействие с ГосСОПКА (3 часа)
1.5	**Разработка памятки для сотрудников «Правила работы с ПДн».** Разработайте памятку для рядовых сотрудников организации (не IT-специалистов) по работе с персональными данными. Включите разделы: 1) Что такое ПДн и зачем их защищать (кратко); 2) Запреты (не передавать, не копировать, не публиковать, не оставлять без присмотра); 3) Правила работы с паролями (сложность, хранение, смена); 4) Действия при подозрительных событиях (странное письмо, потеря телефона/ноутбука, подозрительная активность); 5) Контакт ответственного за ПДн (куда звонить/писать). Объем — 1 страница (четко, понятно, без сложной терминологии, с инфографикой) (2 часа). **Анализ изменений 2026 года: сценарий перехода с Приказа № 21 на новый подход.** Составить пошаговый план перехода для оператора, который ранее работал по Приказу № 21

	(таблицы УЗ-1 - УЗ-4), а с 01.09.2026 переходит на новый риск-ориентированный подход. План должен включать: 1) Анализ текущей системы защиты (инвентаризация ИСПДн, мер, документации); 2) Определение уровня зрелости защиты информации (УЗИ) на основе методики; 3) Пересмотр модели угроз (без обязательной разработки, но с определением актуальных угроз); 4) Корректировку Перечня мер (выбор из нового перечня); 5) Пересмотр договоров с подрядчиками (включение требований по уровню зрелости); 6) Организацию взаимодействия с ГосСОПКА; 7) Обучение персонала новым требованиям. Временные рамки - до 01.09.2026. Оформить в виде дорожной карты (2 часа). **Разработка регламента уничтожения ПДн.** На основе требований 152-ФЗ и Постановления № 687 разработать Регламент уничтожения персональных данных для организации. Документ должен содержать: условия и основания для уничтожения (истечение срока, отзыв согласия, решение суда), состав комиссии, порядок уничтожения для бумажных носителей (способы — шредер, сжигание, пульпа), для электронных носителей (физическое разрушение, перезапись, дегауссинг), для баз данных (процедура удаления записей с подтверждением). Включить форму Акта об уничтожении (2 часа)

3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы включает промежуточную и итоговую аттестацию обучающихся.

3.1 Формы текущей и итоговой аттестации

Текущая аттестация проводится по результатам выполнения практических заданий.

Итоговая аттестация проводится в форме зачета.

Итоговая аттестация осуществляется преподавателем программы на основе двухбалльной («зачтено», «не зачтено») системе оценок.

3.2 Оценочные материалы

Примерный тест для итоговой аттестации по программе «Обеспечение информационной безопасности в автоматизированных системах»

Инструкция: Выберите один или несколько правильных ответов.

1. Каким федеральным законом регулируются отношения в сфере обработки персональных данных в РФ?

а) 149-ФЗ «Об информации...».

б) 152-ФЗ «О персональных данных».

в) 187-ФЗ «О безопасности КИИ».

г) 273-ФЗ «Об образовании».

2. В соответствии с Федеральным законом от 26.07.2026 № 265-ФЗ, какие изменения внесены в 152-ФЗ?

а) Введена обязательная сертификация всех операторов ПДн.

б) Изменены требования к трансграничной передаче ПДн (ст. 12).

в) Отменена обязанность уведомлять Роскомнадзор.

г) Введен запрет на обработку биометрических ПДн.

3. Какой приказ ФСТЭК планируется отменить с 1 сентября 2026 года?

а) Приказ № 17.

б) Приказ № 21.

в) Приказ № 31.

г) Приказ № 117.

4. Какой документ заменяет методику оценки угроз 2008 года согласно требованиям ФСТЭК?

а) Методика оценки угроз 2015 года.

б) Методика оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021).

в) Базовый стандарт защиты информации 2019.

г) Методика оценки ущерба 2020.

5. Кто является субъектом персональных данных?

а) Организация, обрабатывающая данные.

б) Лицо, к которому относятся обрабатываемые данные.

в) Государственный орган, контролирующий обработку.

г) Сотрудник службы безопасности.

6. В течение какого времени оператор обязан уведомить Роскомнадзор об инциденте утечки персональных данных?

а) 72 часа.

б) 24 часа.

в) 3 рабочих дня.

г) 7 дней.

7. Что из перечисленного является одной из ключевых новаций проекта нового приказа ФСТЭК (вместо № 21)?

а) Отмена всех требований к защите ПДн.

б) Введение показателя «уровень зрелости защиты информации».

в) Упрощение требований для государственных систем.

г) Отмена обязательности сертифицированных СЗИ.

8. Какая категория ПДн относится к специальным по 152-ФЗ?

а) ИНН.

б) СНИЛС.

в) Данные о национальной принадлежности.

г) Адрес проживания.

9. Какие новые технологические направления впервые закреплены в проекте нового приказа ФСТЭК?

а) Искусственный интеллект, IoT, облака, API.

б) Только обработка бумажных носителей.

в) Только защита электронной почты.

г) Только шифрование данных.

10. Какая мера является ОРГАНИЗАЦИОННОЙ мерой защиты ПДн?

а) Установка межсетевого экрана.

б) Внедрение СКЗИ.

в) Назначение ответственного за организацию обработки ПДн.

г) Настройка антивируса.

11. Что такое частная модель угроз безопасности ПДн?

а) Утвержденный ФСТЭК перечень всех возможных угроз.

б) Перечень угроз, актуальных для конкретной ИСПДн с учетом ее особенностей.

в) Модель угроз для государственных информационных систем.

г) Документ, не требующий утверждения руководителем.

12. В чем суть риск-ориентированного подхода ФСТЭК, предлагаемого в новом проекте приказа?

а) Все операторы получают единый перечень обязательных мер.

б) Оператор самостоятельно определяет меры защиты на основе оценки рисков и актуальных угроз.

в) Средства защиты выбираются только по рекомендации ФСТЭК.

г) Защита ПДн больше не требуется.

13. Какое действие необходимо выполнить при достижении целей обработки ПДн?

а) Заархивировать все данные на внешний носитель.

б) Уничтожить ПДн (или обеспечить их обезличивание), если иное не предусмотрено законом.

в) Передать данные в Роскомнадзор.

г) Продолжить обработку на усмотрение оператора.

14. Какой способ подачи уведомления об обработке ПДн в Роскомнадзор НЕ является допустимым?

а) Через ЕСИА (Госуслуги) в электронном виде.

б) С использованием ЭЦП.

в) По телефону.

г) На бумажном носителе в территориальный орган.

15. Что из перечисленного является обязанностью оператора ПДн по ст. 18.1 152-ФЗ?

а) Получить лицензию ФСБ на обработку любых ПДн.

б) Назначить лицо, ответственное за организацию обработки ПДн.

в) Ежегодно проходить проверку ФСТЭК.

г) Получить согласие Роскомнадзора на каждую операцию.

Критерии оценки итоговой аттестационной работы:

Оценка	***Критерии оценки***
«зачтено»	Обучающимся дано 60% правильных ответов
«не зачтено»	Обучающимся дано менее 60% правильных ответов

Примерные практические задания для текущей аттестации:

Тема 1.1 Правовое, нормативное и методическое обеспечение безопасности персональных данных

«Правовой аудит организации-оператора с учетом изменений 2026 года»

Цель задания: Научиться проводить комплексный анализ деятельности организации на предмет соответствия требованиям 152-ФЗ (актуальная редакция 2026 г.), определять перечень первоочередных мер и оценивать риски трансграничной передачи.

Описание кейса:

ООО «ТехноСервис» — российская компания по ремонту бытовой техники. Штат - 45 человек. Деятельность:

Кадровый учет: приказы о приеме/увольнении, трудовые договоры, личные карточки Т-2 - бумажные и в 1С:Зарплата и Управление Персоналом.

Клиентская база: форма заявки на сайте (ФИО, телефон, адрес, марка техники, текст поломки) → автоматически попадает в облачную CRM AmoCRM (серверы в РФ).

Мастера: заполняют акты выполненных работ с ФИО клиента, стоимостью, подписью (бумажные документы, хранятся 5 лет).

Пропускная система: отпечатки пальцев сотрудников для входа в офис (биометрические ПДн), данные хранятся в локальной СУБД на контроллере.

Трансграничная передача: компания использует корпоративную почту на Google Workspace для переписки с клиентами и партнерами (на серверах за пределами РФ).

Согласия на обработку ПДн: у клиентов берутся согласия на обработку в бумажной форме в офисе; на сайте согласия через галочку (выразительное действие).

Задача (пошагово):

1. **Определите категории обрабатываемых персональных данных** согласно классификации 152-ФЗ:

- «Иные» ПДн (ФИО, телефон, адрес, должность) - перечислите все.
- «Специальные» ПДн (если есть) - какие именно?
- «Биометрические» ПДн (какие именно?).
- Аргументируйте ссылками на конкретные статьи 152-ФЗ.

2. **Оцените необходимость уведомления Роскомнадзора об обработке ПДн** (ст. 22 152-ФЗ):

Определите, подпадает ли компания под исключения из обязанности уведомления (ст. 22 ч. 2).

Если нужно - заполните форму уведомления (форма № 1) по каждой из 4-х ИСПДн (1С, CRM, почта, пропускная система).

Укажите, какой способ подачи предпочтительнее для данной компании и почему (через ЕСИА, с ЭЦП, на бумаге).

3. **Оцените риски трансграничной передачи ПДн** с учетом Федерального закона от 26.07.2026 № 265-ФЗ:

Является ли использование Google Workspace трансграничной передачей (ст. 12 152-ФЗ)?

Какие требования предъявляются к такой передаче (уведомление РКН, согласие субъекта, оценка адекватности защиты прав субъектов)?

Составьте план действий по легализации использования иностранного облачного сервиса с учетом новой редакции ст. 12 152-ФЗ (укажите конкретные шаги и сроки).

4. **Составьте перечень обязанностей оператора** (ст. 18.1 152-ФЗ) с учетом того, что компания не имеет разработанной документации по ПДн (кроме бумажных согласий). Разделите на:

Меры, которые необходимо внедрить срочно (в течение 1 месяца).

Меры - в перспективе (до 1 года).

Меры - с учетом перехода на новый приказ ФСТЭК с 01.09.2026 (укажите, какие именно).

5. **Разработайте акт оценки вреда субъектам ПДн** (шаблон) для данной организации на основании методики Роскомнадзора. Укажите, является ли вред значительным, и обоснуйте.

Тема 1.2 Угрозы безопасности информационных систем персональных данных

«Разработка частной модели угроз с использованием БДУ ФСТЭК»

Цель задания: Научиться применять актуальную методику оценки угроз ФСТЭК (2021 г.) и Банк данных угроз (БДУ) для построения частной модели угроз для конкретной ИСПДн.

Описание кейса:

Компания «МедАссист» - частная медицинская клиника (15 врачей, 3 администратора, 1 IT-специалист). Используется медицинская информационная система (МИС) «Инфоклиника» с данными:

- Паспортные данные пациентов (серия, номер, кем выдан).
- Данные о состоянии здоровья (диагнозы, результаты анализов, назначения) - специальные ПДн согласно 152-ФЗ.
- СНИЛС, полисы ОМС (номер, страховой полис).
- Контактные данные (телефон, e-mail, адрес).

Инфраструктура:

- Сервер МИС в локальной сети клиники (Windows Server 2022, СУБД PostgreSQL).
- Доступ - только через тонкие клиенты в клинике (удаленный доступ извне закрыт межсетевым экраном).
- Резервное копирование - на внешний жесткий диск ежедневно, диск хранится в той же серверной комнате (без шифрования).
- Врачи используют планшеты (Android) для просмотра результатов анализов в палатах (Wi-Fi, защищенный WPA2-Enterprise, но без сертификатов).
- Клиенты записываются через сайт (форма онлайн-записи - данные передаются по HTTPS).
- В клинике работает 3 администратора, которые имеют доступ ко всем данным пациентов. IT-специалист имеет права администратора на сервере.

Задача (пошагово):

1. **Определите уровень защищенности ИСПДн** согласно Приказу ФСТЭК № 21 и Постановлению № 1119 (до 01.09.2026) и, альтернативно, какой «уровень зрелости» (УЗИ) мог бы быть присвоен по проекту нового приказа (укажите предположительный уровень и обоснуйте).

2. **Используя Банк данных угроз ФСТЭК (БДУ) и Методику оценки угроз 2021 года, составьте перечень актуальных угроз (не менее 12)**. Для каждой угрозы заполните таблицу (пример):

№ п/п	Угроза (номер из БДУ)	Наименование угрозы	Источник угрозы (внешний/внутренний)	Нарушаемый аспект (C/I/A)	Обоснование актуальности для данного кейса
1	УБИ. 001	Несанкционированный доступ к СУБД через эксплуатацию уязвимости	Внешний (хакер)	Конфиденциальность	Необновляемая СУБД, есть риск атаки через интернет
...	...	...	...	...	...

3. **Проведите оценку возможного вреда субъектам ПДн -** определите, является ли вред значительным (материальный, моральный вред), используя методику Роскомнадзора. Учитывайте, что обрабатываются специальные ПДн (состояние здоровья).

4. **Разработайте частную модель угроз** в виде полноценного документа (введение, перечень угроз с обоснованием, выводы). Укажите, что данная модель может быть использована как основа для выбора мер защиты (согласно Приказу № 21 и проектному подходу).

5. **Дополнительно:** укажите, какие 3-4 угрозы являются критическими и требуют первоочередных мер защиты. Кратко предложите меры для них.

Тема 1.3 Организация обработки персональных данных «Разработка полного пакета локальных нормативных актов для оператора»

Цель задания: Овладеть навыками разработки всего комплекта внутренней документации по обработке и защите ПДн в соответствии с требованиями 152-ФЗ.

Описание кейса:

АО «СтройИнвест» - строительная компания с филиалами в 5 городах. Штат - 250 человек. Обрабатывает:

- ПДн сотрудников (кадровый учет, зарплата, налоговые вычеты) - в 1С:Зарплата и управление персоналом.
- ПДн клиентов (договоры долевого участия - паспорт, СНИЛС, адрес, телефон) - в отдельной ИС «Долевик» (разработана на заказ).
- ПДн поставщиков и контрагентов - в той же системе.

Используются:

- 1С:Управление строительной организацией (сервер в ЦОД, доступ по RDP с двухфакторной аутентификацией).
- Битрикс24 (корпоративный портал для внутренней коммуникации, без ПДн).
- Собственная электронная почта на домене (Exchange Server).
- На всех АРМ установлен антивирус Kaspersky.

Ранее документация по ПДн не разрабатывалась (кроме трудовых договоров и согласий клиентов в виде оферты на сайте). Компания готовится к внеплановой проверке Роскомнадзора.

Задача (комплексная):

Разработать следующие документы (каждый - готовый к утверждению проект):

1. **Политика обработки персональных данных** (ПОПДн) — основной документ согласно ст. 18.1 152-ФЗ. Обязательные разделы:

Цели и правовые основания обработки (с указанием конкретных статей 152-ФЗ и иных законов - ТК РФ, ГК РФ).

Перечень обрабатываемых ПДн (с разбивкой по группам субъектов: сотрудники, клиенты, поставщики, контрагенты).

Права субъектов ПДн (с отсылкой к ст. 14 152-ФЗ).

Порядок получения, обработки и уничтожения ПДн.

Перечень применяемых мер защиты (общая формулировка).

2. **Перечень мер, необходимых для обеспечения выполнения обязанностей оператора -** детальный план с указанием:

Конкретных организационных мероприятий (назначение ответственных, издание приказов, обучение, внутренний контроль).

Технических мер (использование СЗИ от НСД, антивирусов, межсетевых экранов, СКЗИ - с указанием конкретных продуктов и мест установки).

Сроков внедрения (для каждой меры - запланированная дата).

Ответственных лиц (должности).

Отметка о наличии сертификации средств (ФСТЭК/ФСБ).

3. **Инструкция пользователя ИСПДн -** для рядовых сотрудников (менеджеры, бухгалтеры, кадровики):

Правила работы с системой, содержащей ПДн.

Запреты (копирование, пересылка по электронной почте без шифрования, печать ПДн без разрешения).

Порядок действий при утере учетных данных, при обнаружении подозрительной активности.

Ответственность за нарушение.

4. **Инструкция администратора информационной системы -** для системного администратора:

Порядок создания/блокировки учетных записей (заявка, согласование).

Настройка политик паролей и прав доступа (минимальные привилегии).

Регламент резервного копирования и восстановления (что, как часто, где хранится, как проверяется).

Порядок регистрации событий безопасности и анализа журналов (какие события аудита включены, как часто проверяются).

Действия при инцидентах (эскалация, изоляция, уведомление).

5. **Положение о внутреннем контроле защиты ПДн**:

Состав комиссии (внутренней или с привлечением внешних экспертов).

Периодичность плановых проверок (не реже 1 раза в год).

Основания для внеплановых проверок (инциденты, смена руководства, изменения в законодательстве).

Перечень проверяемых документов и систем.

Форма акта проверки (результат).

Дополнительное задание:

Подготовьте пояснительную записку для руководства АО «СтройИнвест» (объем 1-2 страницы) о том, как изменится документационная нагрузка с переходом на новый приказ ФСТЭК с 01.09.2026. Какие документы останутся обязательными, какие можно пересмотреть (например, отмена обязательной модели угроз, но не отмена перечня мер).

Тема 1.4 Основы организации и ведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн «Проектирование системы защиты ПДн с учетом риск-ориентированного подхода»

Цель задания: Получить навыки проектирования комплексной системы защиты ПДн на основе нового риск-ориентированного подхода ФСТЭК (проект приказа 2026 года).

Описание кейса:

АО «РосАвто» - дилерский центр по продаже автомобилей. 3 офиса (Москва, Казань, Новосибирск), 200 сотрудников. Обрабатывает:

- ПДн клиентов (ФИО, паспорт, СНИЛС, телефон, адрес) - при продаже автомобилей и оформлении кредитов.
- ПДн сотрудников (кадры, зарплата, налоговые данные).
- Коммерческую тайну (цены, условия поставок, маржинальность).

Инфраструктура:

- Москва: серверная с AD, 1С, файловый сервер (все на Windows Server).
- Удаленные офисы - VPN-подключение к Москве (Cisco AnyConnect).
- Битрикс24 для внутренней коммуникации.
- Удаленные сотрудники (менеджеры) - ноутбуки с VPN.
- Используется корпоративная почта на Exchange Online (Microsoft 365).
- СЗИ от НСД - не используются (только антивирус Kaspersky на всех ПК).
- Резервное копирование - на NAS в Москве (без шифрования) и в облако (Yandex Cloud) раз в неделю.

Компания готовится к переходу на новый приказ ФСТЭК с 01.09.2026.

Задача (комплексная):

1. **Определите актуальные угрозы** для данной инфраструктуры (не менее 12), используя БДУ ФСТЭК. Сделайте акцент на угрозах, связанных с удаленным доступом, облачными сервисами и филиальной сетью.

2. **Проведите упрощенную качественную оценку рисков** для каждой угрозы по шкале «Вероятность: Низкая/Средняя/Высокая» × «Влияние: Низкое/Среднее/Высокое» и определите приоритетные (с высоким риском) — не менее 5 угроз, которые требуют первоочередных мер.

3. **Разработайте концепцию системы защиты** с учетом нового риск-ориентированного подхода (проект приказа ФСТЭК 2026 г.):

Организационные мероприятия - выберите из 21-го мероприятия проекта нового приказа те, которые применимы к данному кейсу (не менее 12). Для каждого укажите, как и когда будет реализовано.

Технические меры - выберите из 17 групп технических мер проекта нового приказа те, которые необходимы (не менее 10 групп). Для каждой укажите, где и как реализуется.

Обоснуйте выбор каждой меры привязкой к конкретной угрозе (из п. 2).

4. **Нарисуйте схему защищенной архитектуры** (можно текстовое описание + блок-схема, либо в Visio):

Разделение на сегменты (DMZ для веб-серверов, внутренняя сеть, сеть удаленных офисов).

Размещение СЗИ, СКЗИ, межсетевых экранов, SIEM-системы (или хотя бы системы сбора логов).

Организация удаленного доступа (VPN с двухфакторной аутентификацией).

Как защищены резервные копии (шифрование, хранение в разных локациях).

5. **Составьте план перехода** с текущего состояния (где почти нет защиты, кроме антивируса и VPN) на новый риск-ориентированный подход до 01.09.2026. Включите этапы:

Проведение аудита и инвентаризация.

Определение уровня зрелости (УЗИ).

Пересмотр модели угроз (без обязательной разработки, но с определением актуальных угроз).

Выбор и закупка сертифицированных СЗИ/СКЗИ.

Внедрение мер (пилотный проект на головном офисе, затем масштабирование).

Пересмотр договоров с подрядчиками (включение требований по уровню зрелости).

Интеграция с ГосСОПКА.

Обучение персонала и внутренний контроль.

Тема 1.5 Методы защиты информационных систем персональных данных «Реагирование на инцидент и переход на новые требования 2026 года»

Цель задания: Отработать алгоритм действий при утечке ПДн с учетом новых требований 2026 года (взаимодействие с ГосСОПКА, сквозной контроль подрядчиков, уровень зрелости).

Описание кейса:

АО «РосАвто» (из предыдущего кейса). 15 мая 2026 года в 10:00 утра специалист по ИБ обнаружил в открытом доступе на теневом сайте (в даркнете) базу данных клиентов за 2024-2025 гг. - 25 000 записей (ФИО, паспорт (серия, номер), телефон, адрес, марка авто, VIN). Установлено, что утечка произошла через уязвимость в старой версии Битрикс24 (не обновлялась 1,5 года, уязвимость была опубликована 6 месяцев назад). В компании нет разработанного плана реагирования на инциденты. Договор с разработчиком Битрикс24 не содержит требований по уровню зрелости.

Задача (комплексная):

1. **Сформируйте экстренный штаб** по реагированию на инцидент. Перечислите должности (минимум 5) и зоны ответственности каждого (юрист, технарь, PR, руководитель, ответственный за ПДн).
2. **Составьте пошаговый план действий по часам** (первые 72 часа):

0-1 час: Локализация, изоляция скомпрометированной системы (отключение от сети), сбор артефактов (дампы, логи, дата-время).

1-4 часа: Предварительный анализ логов, определение вектора атаки и точного объема утечки (сколько записей, какие категории ПДн).

4-24 часа: Заполнение и направление уведомления в Роскомнадзор (форма Приказа № 274) - с указанием, что утечка произошла, и предварительными данными.

24-72 часа: Разработка и направление уведомления субъектам ПДн (текст уведомления - образец, способ доставки - e-mail, СМС, письмо). Составление внутреннего акта расследования (проект).

3. **Учтите новые требования 2026 года:**

Как и когда вы уведомите ГосСОПКА (согласно новым требованиям проекта приказа ФСТЭК)? Какой канал связи используете?

Если утечка произошла через подрядчика (необновленный Битрикс24 - разработчик не предупредил об уязвимости), как вы примените «сквозной контроль подрядчиков»? Что вы сделаете в будущем (оценка уровня зрелости до заключения договора, требования в договоре)?

Как это повлияет на уровень зрелости (УЗИ) компании при следующей оценке?

4. **Составьте итоговый акт расследования** инцидента, в котором:

Описана хронология событий (с датами и временем).

Установлена причина (необновленное ПО, отсутствие мониторинга уязвимостей).

Перечислены нарушения законодательства (какие статьи 152-ФЗ нарушены, какие требования КоАП РФ могут быть применены).

Разработаны корректирующие меры (не менее 5 технических + 5 организационных) с указанием сроков и ответственных.

5. **Разработайте план мероприятий** по недопущению повторных инцидентов с учетом:

Перехода на новый риск-ориентированный подход ФСТЭК (с 01.09.2026).

Пересмотра договоров с подрядчиками (включение требований по уровню зрелости, ответственности за уязвимости).

Повышения уровня зрелости защиты информации (УЗИ) до целевого уровня (какой, по вашему мнению, должен быть у «РосАвто» после инцидента? И какой УЗИ был бы до инцидента?).

Организации регулярного сканирования уязвимостей и пентестов.

Общие критерии оценки практических заданий:

Оценка	***Критерии оценки***
«Отлично»	Задание выполнено полностью, корректно, предложены нестандартные/оптимальные решения. Отчет представлен четко
«Хорошо»	Задание выполнено с незначительными недочетами. Основная цель достигнута.
«Удовлетворительно»	Задание выполнено частично, с ошибками, но общий подход понятен.
«Неудовлетворительно»	Задание не выполнено или выполнено с критическими ошибками, демонстрирующими непонимание темы.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

4.1. Требования к квалификации педагогических кадров

Реализацию программы повышения квалификации осуществляют педагогические работники кафедры «Машиностроение и информационные технологии», имеющие профильное высшее образование и (или) ученую степень, ученое звание, профессиональную переподготовку по профилю программы и (или) привлеченные ведущие специалисты предприятий и организаций, осуществляющие профессиональную деятельность в предметной области программы.

4.2. Материально-технические условия реализации программы

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
Аудитория № 204, 209	Лекционные и практические занятия	Учебная мебель, проектор - 1 шт., персональный компьютер — 11 шт. с доступом к сети «Интернет» и обеспечением доступа в электронную

		информационно-образовательную среду организации. Виртуальные машины с ОС Windows/Linux. Специализированное ПО: КриптоПро CSP (демо-версия), Secret Net (демо), Wireshark (для анализа трафика).

4.3. Учебно-методическое обеспечение программы

Основная литература:

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. - 2-е изд. - Саратов : Вузовское образование, 2024. - 214 c. - ISBN 978-5-4487-1026-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/142805.html.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 3-е изд. - Саратов : Профобразование, 2024. - 702 c. - ISBN 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.iprbookshop.ru/145912.html.

3. Романов, О. О. Техническая защита информации : учебное пособие / О. О. Романов. - Москва: МИСИС, 2023. - 62 с. - ISBN 978-5-907560-61-3. - Текст: электронный//IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/135446.html.

Нормативно-правовые акты (справочные материалы):

- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.04.2024) «О персональных данных».
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.04.2023) «Об утверждении Состава и содержания организационных и технических мер...».
- Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к средствам защиты информации».
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Требований к СКЗИ...».
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн...».
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
- Федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи».
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации, 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными

правовыми актами, операторами, являющимися государственными или муниципальными органами».

- Постановление Правительства Российской Федерации, 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства Российской Федерации, 15 сентября 2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
- Приказ Федеральной службы безопасности России, 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
- Приказ Федеральной службы по техническому и экспортному контролю России, 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную информационных системах». тайну, содержащейся в государственных
- Приказ Федеральной службы по техническому и экспортному контролю России, 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Перечень ресурсов информационно-коммуникационной сети Интернет

1. Электронно-библиотечная система IPRbooks http://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова Web ИРБИС http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN=IBIS
3. Национальная электронная библиотека - http://нэб.рф.
4. Мировая цифровая библиотека - http://www.wdl.org/ru/
5. Международный индекс научного цитирования Web of Science – http://webofscience.com.

6. Научная электронная библиотека eLIBRARY.RU - https://elibrary.ru/defaultx.asp

7. Информационно-правовой портал Гарант – http://www.garant.ru

8. Официальный сайт компании – КонсультантПлюс». http://www.consultant.ru

9. Официальный сайт Федеральной службы по техническому и экспортному контролю – fstec.ru

10. Официальный сайт Федеральной службы безопасности – http://www.fsb.ru

11. Официальный сайт Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций – URL: http://rkn.gov.ru

5. РУКОВОДСТВО И СОСТАВИТЕЛИ ПРОГРАММЫ

Руководитель программы:

Горбушин Алексей Геннадьевич, к.п.н, доцент, доцент кафедры «Машиностроение и информационные технологии», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».

Составители программы:

Пронина Ирина Викторовна, к.э.н., доцент, доцент кафедры «Экономика и менеджмент», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».

Горбушин Алексей Геннадьевич, к.п.н, доцент, доцент кафедры «Машиностроение и информационные технологии», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».