ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)

УТВЕРЖДАЮ
Директор ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)
_____ С.И. Василиади
«10» января 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Защищённая обработка персональных данных, в том числе с использованием средств криптографической защиты информации»

Вид: дополнительная профессиональная программа повышения квалификации.

Показатель	Значение
Объём	42 учебных часов
Форма обучения	Заочная, с применением электронного обучения и дистанционных образовательных технологий
Способ реализации	Дистанционно: электронные материалы, консультации, практические задания и дистанционный контроль
Категория слушателей	Работники, ответственные за обработку персональных данных, специалисты ИБ, администраторы информационных систем персональных данных.
Порядок допуска	Лица, имеющие или получающие среднее профессиональное и (или) высшее образование (ч. 3 ст. 76 № 273-ФЗ).
Итоговый документ	Удостоверение о повышении квалификации при успешной итоговой аттестации

1. Общая характеристика и цель

Цель: Совершенствование компетенций по правомерной обработке персональных данных и применению организационных, технических и криптографических мер защиты.

Продолжительность и учебный график устанавливаются настоящей программой; даты проведения занятий определяются расписанием конкретной группы. Учёт трудоёмкости ведётся в учебных часах. Для занятий применяется академический час 45 минут.

Нормативная основа: Федеральный закон от 29.12.2012 № 273-ФЗ; приказ Минобрнауки России от 24.03.2025 № 266; постановление Правительства РФ от 11.10.2023 № 1678. Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024) применяется в части специальных требований к ДПП в области информационной безопасности.

Содержание учитывает характер профессиональной деятельности и необходимые квалификационные требования к заявленной категории слушателей; освоение программы не присваивает новую квалификацию.

2. Планируемые результаты

Формируемые и совершенствуемые компетенции:

- ПК1. Определять организационные обязанности при обработке персональных данных.
- ПК2. Планировать и реализовывать меры защиты персональных данных в ИСПДн.
- ПК3. Организовывать безопасное применение СКЗИ и реагирование на нарушения безопасности ПДн.

По завершении обучения слушатель должен знать: обязанности оператора персональных данных, требования к ИСПДн, назначение СКЗИ, порядок управления ключевыми носителями и учета инцидентов.

По завершении обучения слушатель должен уметь: проверять состав локальных актов, определять базовые меры защиты, формировать правила использования СКЗИ и оформлять первичное сообщение об инциденте.

3. Учебный план

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
1	Правовые основы обработки ПДн	8	3	3	2	Текущий контроль
2	ИСПДн и требования к защите	10	3	4	3	Текущий контроль
3	Организационная и техническая защита	8	3	3	2	Текущий контроль
4	Применение криптографической защиты	10	3	4	3	Текущий контроль
5	Реагирование на инциденты	4	1	2	1	Текущий контроль
	Итоговая аттестация	2	0	2	0	Тест и кейс
	ВСЕГО	42	13	18	11	

Теор. — теоретическое освоение материала; практ. — практические занятия и задания с обратной связью; самост. — самостоятельная работа. Итоговый контроль включён в общую трудоёмкость.

4. Календарный учебный график

Период	Объём, ч.	Модули/контроль (№ и часы)
Неделя 1	30	1 (8 ч.); 2 (10 ч.); 3 (8 ч.); 4 (4 ч.)
Неделя 2	12	4 (6 ч.); 5 (4 ч.); 6 (2 ч.)

График рассчитан из условной нагрузки не более 30 учебных часов в неделю. При формировании учебной группы конкретные даты и распределение занятий утверждаются расписанием без изменения общей трудоёмкости и итоговых результатов.

5. Рабочие программы дисциплин (модулей)

Модуль 1. Правовые основы обработки ПДн — 8 ч.

Содержание: Принципы обработки и законные основания; Права субъектов и обязанности оператора; Локальные акты, учет операций и ответственность.

Практическая работа: Проверить учебный регламент обработки ПДн.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 2. ИСПДн и требования к защите — 10 ч.

Содержание: Инвентаризация процессов и ИСПДн; Угрозы безопасности и выбор защитных мер; Управление доступом и контроль действий пользователей.

Практическая работа: Составить перечень мер для типового процесса обработки.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 3. Организационная и техническая защита — 8 ч.

Содержание: Полномочия работников и разграничение доступа; Безопасная передача, хранение и уничтожение; Контроль и периодический пересмотр мер.

Практическая работа: Подготовить короткую инструкцию сотрудника.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 4. Применение криптографической защиты — 10 ч.

Содержание: Сценарии применения СКЗИ; Управление ключами, носителями и сертификатами; Типовые нарушения и безопасная эксплуатация.

Практическая работа: Разобрать учебную процедуру выпуска, хранения и отзыва ключей.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 5. Реагирование на инциденты — 4 ч.

Содержание: Обнаружение неправомерного доступа; Эскалация и фиксация обстоятельств; Корректирующие действия и предупреждение повторения.

Практическая работа: Составить карточку инцидента без реальных ПДн.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

6. Организационно-педагогические условия

Обучение организуется в электронной образовательной среде с индивидуальным доступом слушателя к учебным материалам, заданиям и средствам связи с преподавателем. Взаимодействие возможно синхронно и асинхронно. Результаты работ и контроля фиксируются в электронной среде или в учётных ведомостях.

Кадровое обеспечение: преподаватели (специалисты), имеющие образование, профессиональную подготовку и опыт деятельности, соответствующие тематике преподаваемых модулей; при необходимости привлекаются практикующие специалисты.

Материально-техническое и информационное обеспечение: компьютер с доступом к сети Интернет, программные средства чтения учебных материалов, демонстрационные материалы, тестовая среда и учебные кейсы. Для практических заданий используются учебные данные, демонстрационные конфигурации, симуляторы или специально выделенные стенды по тематике курса.

Методическое обеспечение: конспекты и презентации, нормативные и эксплуатационные материалы из раздела 8, задания для самостоятельной работы, инструкции к практическим работам, контрольные вопросы и критерии оценивания.

Особенности ИБ: программа не предполагает использование сведений, составляющих государственную тайну, либо реальных ключей, паролей и конфиденциальных данных обучающихся или заказчиков. Дистанционно изучаются материалы и выполняются учебные задачи с применением стендов/симуляторов. Если конкретная практическая работа требует физического доступа к защищаемому оборудованию или иного режима, она проводится лишь при обеспечении соответствующих условий; возможность полностью дистанционного освоения проверяется до начала реализации.

Порядок актуализации и передачи: изменения содержания вносятся после проверки применимых требований законодательства и утверждаются директором. Передача программы сторонней образовательной организации допускается по оформленному соглашению с соблюдением прав на материалы и режима доступа; сведения ограниченного доступа в программу не включаются.

7. Контроль результатов и оценочные материалы

Текущий контроль проводится по заданиям модулей с результатом «зачтено/не зачтено». Слушатель получает комментарии к ошибкам и возможность повторного выполнения задания в пределах срока обучения.

Итоговый контроль: дистанционный тест и практико-ориентированный кейс. Тест содержит не менее 10 заданий по содержанию всех модулей. Для положительного результата требуется не менее 70% верных ответов и выполнение ключевых требований практического кейса. Допускается повторная проверка в порядке, предусмотренном локальными актами.

Типовые контрольные вопросы:

1. Какие основные обязанности имеет оператор персональных данных?

2. Зачем ограничивается доступ к ПДн по должностным функциям?

3. Как поступить при обнаружении чужого ключевого носителя?

4. Какие сведения включают в журнал регистрации инцидентов?

5. Чем защита канала передачи отличается от защиты данных на рабочей станции?

Практическое итоговое задание: Для заданной ИСПДн составить краткую карту обработки персональных данных, перечень защитных мер и инструкцию по обращению с ключевыми носителями.

Критерии оценки кейса: (1) корректно выделены исходные условия и риски; (2) действия и документы предложены последовательно; (3) применены уместные технические и организационные меры; (4) не предложены действия, противоречащие требованиям безопасности. Результат «зачтено» — выполнение не менее трёх из четырёх критериев при обязательном соблюдении критерия 4.

Освоение завершается итоговой аттестацией. Успешно прошедшему итоговую аттестацию слушателю выдаётся удостоверение о повышении квалификации в установленном организацией порядке. При неудовлетворительном результате действуют правила выдачи справки об обучении.

8. Основные нормативные и методические источники

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Приказ Минобрнауки России от 24.03.2025 № 266.
- Постановление Правительства РФ от 11.10.2023 № 1678.
- Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024).
- Федеральный закон от 27.07.2006 № 152-ФЗ.
- Постановление Правительства РФ от 01.11.2012 № 1119.
- Применимые действующие нормативные акты ФСТЭК и ФСБ России по защите ПДн и использованию СКЗИ.

Учебные и справочные материалы актуализируются перед реализацией очередной группы с учётом действующих редакций нормативных документов.