ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)

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

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

Вид: дополнительная профессиональная программа повышения квалификации.

Показатель	Значение
Объём	216 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	Специалисты по защите информации, администраторы безопасности, ответственные за организацию защиты информации в информационных системах.
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 организационной и технической защите информации ограниченного доступа без использования сведений, составляющих государственную тайну.

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 нормативные и организационные требования по защите информации ограниченного доступа.
- ПК2. Формировать модель угроз и планировать систему защиты информации.
- ПК3. Выбирать меры и средства технической защиты, осуществлять контроль их внедрения и функционирования.

По завершении обучения слушатель должен знать: правовые основы ТЗИ, модели угроз, структуру организационно-распорядительных документов, категории технических мер и порядок оценки их реализации.

По завершении обучения слушатель должен уметь: обследовать ИС, формировать перечень требований, проектировать комплекс мер защиты и анализировать результаты проверки защищённости.

3. Учебный план

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
1	Правовое регулирование и объекты защиты	30	10	12	8	Текущий контроль
2	Угрозы, нарушитель и оценка рисков	40	14	16	10	Текущий контроль
3	Организационные и технические меры	58	20	23	15	Текущий контроль
4	Эксплуатация и контроль системы защиты	44	15	18	11	Текущий контроль
5	Оценка реализации требований защиты	40	14	16	10	Текущий контроль
	Итоговая аттестация	4	0	4	0	Тест и кейс
	ВСЕГО	216	73	89	54	

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 (30 ч.)
Неделя 2	30	2 (30 ч.)
Неделя 3	30	2 (10 ч.); 3 (20 ч.)
Неделя 4	30	3 (30 ч.)
Неделя 5	30	3 (8 ч.); 4 (22 ч.)
Неделя 6	30	4 (22 ч.); 5 (8 ч.)
Неделя 7	30	5 (30 ч.)
Неделя 8	6	5 (2 ч.); 6 (4 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. Правовое регулирование и объекты защиты — 30 ч.

Содержание: Категории информации ограниченного доступа; Требования регуляторов к защите информации; Определение границ ИС и состава защищаемых ресурсов.

Практическая работа: Сформировать реестр объектов и применимых требований для учебной ИС.

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

Модуль 2. Угрозы, нарушитель и оценка рисков — 40 ч.

Содержание: Инвентаризация активов и каналов взаимодействия; Модель нарушителя и угроз безопасности; Оценка актуальности угроз и приоритизация мер.

Практическая работа: Подготовить фрагмент модели угроз по заданной архитектуре.

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

Модуль 3. Организационные и технические меры — 58 ч.

Содержание: Разграничение доступа и управление учетными записями; Регистрация событий, сетевое разделение и защита конечных точек; Резервное копирование, антивирусная защита и управление уязвимостями.

Практическая работа: Составить проект перечня мер и матрицу ответственности.

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

Модуль 4. Эксплуатация и контроль системы защиты — 44 ч.

Содержание: Эксплуатационная документация и регламентирование; Мониторинг событий, изменения конфигураций и инциденты; Поддержка актуальности организационно-распорядительной документации.

Практическая работа: Разработать регламент контроля выполнения мер защиты.

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

Модуль 5. Оценка реализации требований защиты — 40 ч.

Содержание: Проверка настроек и подтверждающие свидетельства; Программа и методики контрольных испытаний; Формирование выводов и плана корректирующих мероприятий.

Практическая работа: Подготовить отчет о контрольной проверке по учебному сценарию.

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. Как определяется граница защищаемой информационной системы?

2. Чем модель угроз отличается от перечня уязвимостей?

3. Какие документы регламентируют управление доступом?

4. Какими свидетельствами подтверждается выполнение технической меры?

5. Когда нужно пересматривать модель угроз?

Практическое итоговое задание: Для учебной распределенной информационной системы определить состав защищаемых активов, применимые требования, основные угрозы и набор организационно-технических мер с контрольными процедурами.

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).
- Федеральные законы от 27.07.2006 № 149-ФЗ и № 152-ФЗ (по области применения).
- Действующие применимые нормативные акты ФСТЭК России по защите информации в соответствующих видах информационных систем.

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