УТВЕРЖДЕНА приказом ООО «Эдуклайн» от «» _____ 2026 г. № 3

Генеральный директор ООО «Эдуклайн» __ / Волкова А. Л. /

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА — ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение защиты информации в автоматизированных системах»

> ■ **ПРОГРАММА РЕАЛИЗУЕТСЯ ИСКЛЮЧИТЕЛЬНО С ПРИМЕНЕНИЕМ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ (ЭО и ДОТ).** Обучение полностью дистанционное (ст. 16 Федерального закона № 273-ФЗ). Аудиторные занятия с физическим присутствием обучающихся не проводятся; освоение программы обеспечивается в электронной информационно-образовательной среде (ЭИОС) независимо от места нахождения обучающегося.

Объём: 72 академических часа **Форма обучения:** заочная **Образовательные технологии:** программа реализуется исключительно с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ); аудиторные занятия с физическим присутствием обучающихся не проводятся **Документ по итогам:** удостоверение о повышении квалификации

дер. Касимово, Ленинградская область — 2026

1. Общие положения и пояснительная записка

Настоящая дополнительная профессиональная программа — программа повышения квалификации (далее — программа) разработана и утверждена ООО «Эдуклайн» самостоятельно в соответствии с частью 5 статьи 12 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

1.1. Нормативная основа

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (ст. 12, 13, 16, 17, 60, 74, 76);
- Приказ Минобрнауки России от 24.03.2025 № 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (применяется с 01.09.2025);
- Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (код 06.033), утверждённый приказом Минтруда России от 14.09.2022 № 525н (действует с 01.03.2023);
- локальный нормативный акт ООО «Эдуклайн» «Положение о реализации образовательных программ с применением электронного обучения и дистанционных образовательных технологий»;
- локальные нормативные акты Организации об электронной информационно-образовательной среде, о текущем контроле и итоговой аттестации, об идентификации обучающихся.

> Реализация программы с применением ЭО и ДОТ осуществляется на основании **статьи 16 Федерального закона № 273-ФЗ** и указанного локального нормативного акта Организации.

1.2. Цель

Совершенствование профессиональных компетенций обучающихся в рамках имеющейся квалификации, необходимых для обеспечения защиты информации (в том числе персональных данных) в автоматизированных системах, в соответствии с требованиями профессионального стандарта «Специалист по защите информации в автоматизированных системах» (06.033), а также нормативных правовых актов Российской Федерации и методических документов ФСТЭК России и ФСБ России в области защиты информации.

1.3. Категория слушателей

Лица, имеющие или получающие среднее профессиональное и (или) высшее образование. Слушатели, имеющие СПО, совершенствуют компетенции в рамках обобщённой трудовой функции А (уровень квалификации 5) профстандарта 06.033; имеющие ВО — в рамках обобщённой трудовой функции В (уровень квалификации 6).

1.4. Трудоёмкость и срок освоения

72 академических часа. Срок освоения устанавливается расписанием (при непрерывном обучении — до 3 недель); конкретные даты фиксируются приказом о зачислении и в расписании ЭИОС.

1.5. Форма обучения и образовательные технологии

Форма обучения — заочная. Программа реализуется **исключительно с применением электронного обучения и дистанционных образовательных технологий** (ст. 16 Федерального закона № 273-ФЗ). Все виды учебной деятельности, текущий контроль и итоговая аттестация проводятся дистанционно в электронной информационно-образовательной среде (ЭИОС) Организации, независимо от места нахождения слушателя. Аудиторные занятия с физическим присутствием обучающихся не проводятся.

1.6. Ограничения предмета программы

Программа носит общий организационно-технический характер, **не содержит сведений, составляющих государственную тайну**, **не предусматривает работу с реальными средствами криптографической защиты информации (СКЗИ)** и **не требует наличия лицензий ФСБ России или ФСТЭК России**. Криптографические методы рассматриваются исключительно в обзорном (ознакомительном) порядке. В связи с этим ограничения части 5 статьи 16 Федерального закона № 273-ФЗ к программе не применяются, и она может реализовываться исключительно с применением ЭО и ДОТ.

---

2. Планируемые результаты обучения

В результате освоения программы обучающийся **совершенствует** следующие профессиональные компетенции (в рамках имеющейся квалификации), соотнесённые с трудовыми функциями обобщённых трудовых функций А (уровень 5) и В (уровень 6) профстандарта 06.033:

- **ПК-1.** Применять нормативные правовые акты и организационно-распорядительные документы по защите информации в автоматизированных системах.
- **ПК-2.** Выявлять и оценивать угрозы безопасности информации, разрабатывать модель угроз и модель нарушителя.
- **ПК-3.** Применять организационные и технические меры и средства защиты информации в автоматизированных системах (включая средства криптографической защиты — обзорно).

- **ПК-4.** Обеспечивать защиту персональных данных при их обработке в автоматизированных системах в соответствии с законодательством Российской Федерации.
- **ПК-5.** Осуществлять мониторинг событий и реагирование на инциденты информационной безопасности.

2.1. Соответствие результатов профессиональному стандарту 06.033 (таблица)

Совершенствуемая компетенция	ОТФ / ТФ 06.033	Соотнесение (трудовые действия, умения, знания)
ПК-1. Применение НПА и ОРД по защите информации в АС	A, B	Знание НПА и методических документов ФСТЭК/ФСБ России; умение применять требования к защите информации в АС
ПК-2. Выявление и оценка угроз, модель угроз/нарушителя	A (анализ угроз безопасности информации)	Умение выявлять угрозы; знание методик моделирования угроз (БДУ ФСТЭК)
ПК-3. Организационные и технические меры и средства защиты в АС	A, B (настройка и эксплуатация средств защиты)	Трудовые действия по установке, настройке, эксплуатации средств защиты информации
ПК-4. Защита персональных данных в АС	A, B	Знание требований ФЗ-152 и подзаконных актов; умение реализовывать меры защиты ПДн
ПК-5. Мониторинг и реагирование на инциденты ИБ	B (мониторинг инцидентов ИБ)	Трудовые действия по мониторингу событий и обработке инцидентов

Каждая компетенция раскрывается через «знать / уметь / владеть»:

Знать: нормативно-правовую и методическую базу защиты информации в АС; классификацию угроз и модель нарушителя; состав организационных и технических мер и средств защиты; требования к обработке и защите персональных данных; порядок мониторинга и реагирования на инциденты ИБ. **Уметь:** применять требования НПА к защите информации в АС; выявлять и оценивать угрозы, разрабатывать модель угроз; подбирать и настраивать меры и средства защиты; оформлять организационно-распорядительную документацию по ИБ и защите ПДн. **Владеть:** навыками анализа защищённости АС, подготовки документов по защите информации и реагирования на инциденты (в объёме, отрабатываемом на виртуальных стендах ЭИОС).

---

3. Учебный план

№	Наименование раздела (модуля)	Всего, ч	Теория (ЭО/ДОТ)	Практика (виртуальные стенды/задания в ЭИОС)	Форма контроля
1	Правовые и организационные основы защиты информации в АС (ФЗ-149, ФЗ-152, требования ФСТЭК/ФСБ России)	12	6	6	тек. тест
2	Угрозы безопасности информации, модель угроз и нарушителя, оценка рисков	14	6	8	тек. тест
3	Организационные и технические меры и средства защиты информации в АС; криптография (обзорно)	18	8	10	тек. тест
4	Защита персональных данных при обработке в АС, организационно-	12	5	7	тек. тест

№	Наименование раздела (модуля)	Всего, ч	Теория (ЭО/ ДОТ)	Практика (виртуальные стенды/ задания в ЭИОС)	Форма контроля
	распорядительная документация				
5	Практикум: модель угроз, комплект ОРД по защите ПДн, реагирование на инцидент (виртуальные стенды ЭИОС)	12	—	12	зачёт по практикуму
6	**Итоговая аттестация** (итоговое тестирование в ЭИОС)	4	—	4	итоговое тестирование
	ИТОГО	**72**	25	47	

Все виды занятий реализуются дистанционно в ЭИОС (ЭО и ДОТ).

---

4. Календарный учебный график

Обучение проводится в течение всего календарного года по мере комплектования групп. Даты начала и окончания устанавливаются приказом о зачислении. Все виды учебной деятельности реализуются в ЭИОС; при асинхронном формате указываются периоды доступности материалов и контрольные точки. Итоговая аттестация выделяется отдельной контрольной точкой в завершение обучения.

---

5. Рабочие программы разделов (содержание)

Раздел 1. Понятие защиты информации в автоматизированных системах. ФЗ-149 «Об информации…», ФЗ-152 «О персональных данных». Система регуляторов (ФСТЭК, ФСБ, Роскомнадзор). Виды защищаемой информации, режим коммерческой тайны. Организационные основы построения системы защиты информации в АС.

Раздел 2. Классификация угроз и уязвимостей безопасности информации. Модель угроз и модель нарушителя. Банк данных угроз безопасности информации (БДУ) ФСТЭК России. Методики оценки рисков.

Раздел 3. Организационные и технические меры защиты информации в АС. Средства защиты информации (СЗИ от НСД, межсетевые экраны, антивирусная защита, средства обнаружения вторжений). Основы сетевой безопасности. Криптографические методы защиты (обзорно, без работы с реальными СКЗИ).

Раздел 4. Обработка персональных данных в АС: принципы, правовые основания, права субъектов. Обязанности оператора ПДн. Организационно-распорядительная документация по защите ПДн (политики, приказы, инструкции, модель угроз ИСПДн).

Раздел 5. Практикум на виртуальных стендах ЭИОС: разработка модели угроз для условной АС; подготовка комплекта ОРД по защите ПДн; отработка сценария реагирования на инцидент ИБ.

---

6. Организационно-педагогические условия. Реализация программы с применением ЭО и ДОТ

6.1. Электронная информационно-образовательная среда (ЭИОС)

Программа реализуется в ЭИОС Организации — образовательном приложении «Эдуклайн» (личный кабинет обучающегося). ЭИОС обеспечивает: - доступ обучающихся к электронным учебным

материалам (видеолекции, электронные конспекты, презентации, нормативные документы, тренажёры, тестовые задания, виртуальные стенды) в режиме 24/7 независимо от места нахождения; - синхронное (вебинары) и асинхронное взаимодействие обучающегося и преподавателя; - фиксацию хода образовательного процесса, результатов освоения программы и формирование электронных ведомостей; - хранение результатов обучения на электронных носителях.

6.2. Идентификация обучающегося

Идентификация личности обучающегося обеспечивается посредством индивидуальной учётной записи (логин/пароль либо вход через мессенджер по одноразовому коду) в ЭИОС. При прохождении итоговой аттестации личность обучающегося подтверждается сверкой документа, удостоверяющего личность, в режиме видео-конференц-связи (при необходимости — средствами прокторинга). Порядок идентификации установлен локальным нормативным актом Организации.

6.3. Аттестация в дистанционном формате

Текущий контроль, промежуточная и итоговая аттестация проводятся дистанционно в ЭИОС: автоматизированное тестирование, дистанционная защита практикума (загрузка выполненных работ, вебинар). Результаты фиксируются в ЭИОС; по итоговой аттестации оформляется электронная ведомость (протокол).

6.4. Кадровое обеспечение

К реализации программы привлекаются педагогические работники, имеющие профильное образование и (или) профессиональную переподготовку в области информационной безопасности / информационных технологий, соответствующие квалификационным требованиям.

6.5. Учебно-методическое и методическое обеспечение

Электронные конспекты, презентации, видеоматериалы, нормативные документы, методические рекомендации по выполнению практических заданий, тестовые и практические задания размещаются в ЭИОС и доступны обучающимся на весь период обучения.

---

7. Формы аттестации и оценочные материалы

- **Текущий контроль:** тестирование по разделам 1–4 (порог — не менее 60% правильных ответов).
- **Промежуточная аттестация:** зачёт по практикуму (раздел 5) — «зачтено»/«не зачтено».
- **Итоговая аттестация:** итоговое тестирование в ЭИОС (не менее 40 вопросов, порог — 70%). Оценка: «зачтено»/«не зачтено».

Оценочные материалы включают: банк тестовых вопросов (не менее 40) по разделам; критерии оценивания практических работ; описание процедуры дистанционного тестирования и шкалу оценивания. Полный банк оценочных материалов формируется и хранится в ЭИОС.

Лицам, успешно прошедшим итоговую аттестацию, выдаётся **удостоверение о повышении квалификации**; сведения о выданном документе вносятся в ФИС ФРДО в установленный срок.

Пример оценочных материалов (фрагмент банка вопросов): 1. Федеральный закон, регулирующий обработку персональных данных: *(ФЗ-152)*. 2. Орган, устанавливающий требования к защите информации в государственных информационных системах и ИСПДн: *(ФСТЭК России)*. 3. Что входит в модель нарушителя: *(типы, мотивация и возможности потенциальных нарушителей)*.