Министерство образования Кировской области
Кировское областное государственное образовательное автономное учреждение дополнительного профессионального образования
«Институт развития образования Кировской области»
Дополнительная профессиональная программа
(повышение квалификации)

«УТВЕРЖДАЮ»
Ректор ИРО Кировской области
Н.В. Соколова
№ 7 от 23.10.2026

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 708F6F7C1A7645257C387A08A0C2DD1A
Владелец: Соколова Наталья Вячеславовна
Действителен: с 13.01.2026 до 08.04.2027

Основы администрирования автоматизированных рабочих мест, подключенных к государственным информационным системам в сфере образования

Разработчик(и) программы:
Кряжевских Д.А., Кировское областное государственное образовательное автономное учреждение дополнительного профессионального образования
«Институт развития образования Кировской области»

Киров, 2026

Раздел 1. Характеристика программы

1.1. Цель реализации программы – совершенствование компетенций слушателей в сфере эксплуатации и администрирования автоматизированных рабочих мест, подключенных к государственным информационным системам.

1.2. Планируемые результаты обучения:

Системный администратор

Трудовые функции	Трудовые действия	Знать	Уметь
B/04.5 Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ (Профессиональный стандарт 06.026 «Системный администратор информационно-коммуникационных систем»)	Запуск процедуры установки прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании Контроль процедуры установки прикладного программного обеспечения Настройка установленного прикладного программного обеспечения на конечных устройствах пользователей	1) Лицензионные требования по установке и настройке программного обеспечения 2) Программно-аппаратные средства защиты информации автоматизированных систем 3) Мероприятия по организации системы защиты информации в автоматизированных системах	1) Устанавливать и настраивать автоматизированные рабочие места государственных информационных систем без привлечения третьих лиц; 2) Проводить оценку эффективности принятых мер информационной безопасности в соответствии с требованиями законодательства Российской Федерации
B/05.5 Проведение обновления программного обеспечения технических средств информационно-коммуникационных систем по инструкциям производителей (Профессиональный стандарт 06.026 «Системный администратор информационно-коммуникационных систем»)	Мониторинг доступности обновлений программного обеспечения информационно-коммуникационной системы, выпущенных производителем Выполнение обновления программного обеспечения технических средств согласно инструкции	1) Лицензионные требования по установке и настройке программного обеспечения 2) Программно-аппаратные средства защиты информации автоматизированных систем 3) Мероприятия по организации системы защиты информации в автоматизированных системах	1) Устанавливать и настраивать автоматизированные рабочие места государственных информационных систем без привлечения третьих лиц; 2) Проводить оценку эффективности принятых мер информационной безопасности в соответствии с требованиями законодательства Российской Федерации

Специалист по защите информации в автоматизированных системах

A/02.5 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем (Профессиональный стандарт 06.033 «Специалист по защите	Ведение протоколов и журналов учета при изменении конфигурации систем защиты информации автоматизированных систем Ведение протоколов	1) Лицензионные требования по установке и настройке программного обеспечения 2) Программно-аппаратные средства защиты информации	1) Устанавливать и настраивать автоматизированные рабочие места государственных информационных систем без привлечения третьих лиц; 2) Проводить оценку эффективности принятых

информации в автоматизированных системах»)	и журналов учета при осуществлении мониторинга / аудита систем защиты информации автоматизированных систем	автоматизированных систем 3) Мероприятия по организации системы защиты информации в автоматизированных системах	мер информационной безопасности в соответствии с требованиями законодательства Российской Федерации
B/02.6 Администрирование систем защиты информации автоматизированных систем (Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах»)	Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	1) Лицензионные требования по установке и настройке программного обеспечения 2) Программно-аппаратные средства защиты информации автоматизированных систем 3) Мероприятия по организации системы защиты информации в автоматизированных системах	1) Устанавливать и настраивать автоматизированные рабочие места государственных информационных систем без привлечения третьих лиц; 2) Проводить оценку эффективности принятых мер информационной безопасности в соответствии с требованиями законодательства Российской Федерации
B/06.6 Аудит защищенности информации в автоматизированных системах (Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах»)	Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем Экспертиза состояния защищенности информации автоматизированных систем	1) Лицензионные требования по установке и настройке программного обеспечения 2) Программно-аппаратные средства защиты информации автоматизированных систем 3) Мероприятия по организации системы защиты информации в автоматизированных системах	1) Устанавливать и настраивать автоматизированные рабочие места государственных информационных систем без привлечения третьих лиц; 2) Проводить оценку эффективности принятых мер информационной безопасности в соответствии с требованиями законодательства Российской Федерации

1.3. Категория слушателей: Системный администратор информационно-коммуникационных систем, специалист по защите информации в автоматизированных системах или лица, выполняющие функции данных специалистов

1.4. Форма обучения – очно-заочная с применением ДОТ.

1.5. Срок освоения программы: 16 ч.

Раздел 2. Содержание программы

2.1. Учебно-тематический план

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ			Формы контроля
			Лекция, час	Интерактивное (практическое) занятие, час	Самостоятельная работа	
1.	**Входное тестирование**	**1**	**0**	**0**	**1**	**Тестирование**
2.	**Актуальные требования к обеспечению работы образовательных организаций в федеральных и региональных государственных информационных системах**	**2**	**0**	**0**	**2**	
2.1	Организационные и технические требования для подключения образовательных организаций к государственным информационным системам в сфере образования	1	0	0	1	
2.2	Основные инструменты работы в государственных информационных системах в сфере образования	1	0	0	1	
3.	**Порядок настройки и администрирования автоматизированных рабочих мест, подключенных к государственным информационным системам в сфере образования**	**6**	**0**	**6**	**0**	
3.1	Установка и настройка операционной системы на базе Linux	1	0	1	0	
3.2	Организация канала связи и сетевого взаимодействия при передаче и получении информации. Конфиденциальный документооборот	2	0	2	0	
3.3	Организация обнаружения и предотвращения вторжений на сетевом уровне. Сегментация и межсетевое экранирование	1	0	1	0	
3.4	Порядок установки и настройки антивирусного программного обеспечения. Контроль носителей информации	1	0	1	0	
3.5	Работа с обновлениями программного обеспечения на автоматизированных рабочих местах	1	0	1	0	

№ п/п	Наименование разделов (модулей) и тем	Всего часов	Виды учебных занятий, учебных работ			Формы контроля
			Лекция, час	Интерактивное (практическое) занятие, час	Самостоятельная работа	
4.	**Проведение аудита защищенности информации, обрабатываемой на автоматизированных рабочих местах, подключенных к государственным информационным системам**	**6**	**0**	**2**	**4**	
4.1	Ведение организационно - технической документации в области эксплуатации системы защиты информации автоматизированных рабочих мест	3	0	0	3	
4.2	Организация проведения оценки соответствия требованиям безопасности, предъявляемым к автоматизированным рабочим местам, подключенным к государственным информационным системам в сфере образования	3	0	2	1	**Практическая работа**
5.	**Итоговая аттестация**	**1**	**0**	**0**	**1**	**Тестирование**
ИТОГО		**16**	**0**	**8**	**8**	

2.2 Рабочая программа

1. Входное тестирование (самостоятельная работа - 1 ч.)

Проведение входного тестирования по определению уровня знаний слушателей о нормативно-правовых требованиях в области подключения и работы с федеральными и региональными государственными информационными системами в сфере образования, процессах администрирования автоматизированных рабочих мест организации, порядке проведения контроля принятых мер информационной безопасности.

2. Модуль 1. Актуальные требования к обеспечению работы образовательных организаций в федеральных и региональных государственных информационных системах

Тема 1. Организационные и технические требования для подключения образовательных организаций к государственным информационным системам в сфере образования

Самостоятельная работа – 1 час.

Слушатели изучают перспективы цифровой трансформации системы образования Кировской области; состояние развития ИТ сферы системы образования; нормативно-правовые требования в области подключения и работы образовательных организаций в государственных информационных системах; особенности работы в государственных информационных системах и интеграции сведений на витрины данных ЕПГУ.

Тема 2. Основные инструменты работы в государственных информационных системах в сфере образования

Самостоятельная работа – 1 час.

Слушатели изучают виды инструментов работы в государственных информационных системах в сфере образования для: работы с данными и учёта, организации учебного процесса, доступа к верифицированному контенту, коммуникации и взаимодействия. Рассматривают дополнительные инструменты работы в ГИС, организацию процесса авторизации пользователей через ЕСИА и обеспечение эффективной и безопасной работы образовательных организаций в государственных информационных системах.

3. Модуль 2. Порядок настройки и администрирования автоматизированных рабочих мест, подключенных к государственным информационным системам в сфере образования

Тема 1. Установка и настройка операционной системы на базе Linux

Практическое занятие – 1 час.

Слушатели производят установку ОС Linux на персональных компьютерах, установку основных системных сервисов, создание профилей пользователей и пользовательских окружений. Изучают основные команды системы Linux и возможности командного процессора. Результатом занятия является подготовленное автоматизированное рабочее место с установленной ОС и подключенными репозиториями.

Тема 2. Организация канала связи и сетевого взаимодействия при передаче и получении информации. Конфиденциальный документооборот

Практическое занятие – 2 часа.

Слушатели изучают основные функциональные возможности и прикладные системы защиты канала связи на базе комплексов ViPNet и КриптоПРО. Производят установку одного из двух программных комплексов на рабочее место, проверяют доступность сетевых узлов, устанавливают сертификаты центров сертификации и актуальные списки отозванных сертификатов (CRL) удостоверяющего центра, производят проверку настроек безопасности средствами установленных комплексов. Пробуют отправить тестовое письмо посредством модуля конфиденциального документооборота «ViPNet Деловая почта». Результатом занятия является получение доступа к ресурсам государственных информационных систем с установленного рабочего места.

Тема 3. Организация обнаружения и предотвращения вторжений на сетевом уровне. Сегментация и межсетевое экранирование

Практическое занятие – 1 час.

Слушатели изучают организацию межсетевого экранирования: типы и идентификаторы правил, порядок обнаружения и предотвращения вторжений на автоматизированных рабочих местах. Устанавливают и производят настройку на рабочем месте программного обеспечения ViPNet EndPoint Protection: включение модуля межсетевого экрана, включение модуля обнаружения вторжений. Результатом занятия является установленное и функционирующее на рабочем месте средство межсетевого экранирования и обнаружения вторжений, имеющее актуальные базы правил.

Тема 4. Порядок установки и настройки антивирусного программного обеспечения. Контроль носителей информации

Практическое занятие – 1 час.

Слушатели осуществляют установку на рабочем месте антивирусного программного обеспечения на базе решения Kaspersky Endpoint Security. Изучают порядок учета, проверок и обновлений баз сигнатур. Отрабатывают действия при обнаружениях вредоносного программного обеспечения. Устанавливают на рабочем месте следующие настройки безопасности:

Включают опцию «Не обновлять программные модули».

Отключают установку компонента «Сетевой экран».

Включают установка компонента «Контроль устройств».

Отключают установку компонента «Обнаружение вторжений».

Отключают участие в Kaspersky Security Network.

Результатом занятия является установленное и функционирующее на рабочем месте антивирусное программное обеспечение, осуществляющее автоматический контроль съемных носителей информации при подключении.

Тема 5. Работа с обновлениями программного обеспечения на автоматизированных рабочих местах

Практическое занятие – 1 час.

Слушатели изучают регламентные работы по обслуживанию автоматизированных рабочих мест, осуществляемые при взаимодействии и без взаимодействия с оператором государственной информационной системы, анализируют случаи, требующие установки критических обновлений программного обеспечения. Отрабатывают сценарии восстановления рабочих мест после сбоя обновлений и порядок устранения типичных неисправностей, возникающих при эксплуатации рабочих мест. Производят обновление релиза операционной системы на рабочем месте.

4. Модуль 3. Проведение аудита защищенности информации, обрабатываемой на автоматизированных рабочих местах, подключенных к государственным информационным системам

Тема 1. Ведение организационно - технической документации в области эксплуатации системы защиты информации автоматизированных рабочих мест

Самостоятельная работа – 3 часа.

Слушатели изучают перечень локальных актов образовательного учреждения в области обеспечения защиты информации при работе в государственных информационных системах: инструкции, положения, учетную документацию. Анализируют пакет документов, необходимый для подключения организации к защищенной сети и государственной информационной системе.

По результатам изученного материала слушатели осуществляют подготовку и заполнение комплекта отчетной организационно - технической документации для подключения автоматизированного рабочего места организации к РГИС ЕРИСО КО в следующем составе:

1) Заявка на подключение;
2) Анкета;
3) Проект приказа об организации защищенного АРМ;
4) Проект приказа о режиме в помещении с АРМ РГИС ЕРИСО КО;
5) Проект технического паспорта АРМ;
6) Заявка на получение доступа к информационным ресурсам РГИС ЕРИСО КО;
7) Акт ввода в эксплуатацию АРМ РГИС ЕРИСО КО.

Шаги выполнения:

1. В личном кабинете курса выберете один из двух способов подключения рабочего места к РГИС ЕРИСО КО.

с помощью защищенной сети ViPNet;

с помощью виртуальных сетей TLS на базе КриптоПРО.

2. В соответствии с выбранным способом скачайте шаблоны документов для формирования комплекта отчетной организационно - технической документации.

3. Произведите заполнение шаблонов документов в заданном объеме.

Результат выполнения: комплект в составе 7 отчетных документов, заполненный от имени организации, в которой работает слушатель, в целях направления для подключения автоматизированного рабочего места к РГИС ЕРИСО КО.

Тема 2. Организация проведения оценки соответствия требованиям безопасности, предъявляемым к автоматизированным рабочим местам, подключенным к государственным информационным системам в сфере образования

Самостоятельная работа – 1 час.

Слушатели изучают порядок осуществления контроля защищенности автоматизированного рабочего места. Организационные меры защиты информации. Инструктажи ответственных лиц. Ограничение доступа в помещения и к автоматизированным рабочим местам. Требования к допуску и обслуживанию помещений и автоматизированных рабочих мест. Технические меры защиты информации. Состав программного обеспечения на рабочих местах. Проверка настроек безопасности.

Практическое занятие – 2 часа.

Практическая работа № 1: проведение аудита защищенности информации, обрабатываемой на автоматизированном рабочем месте.

Раздел 3. Формы аттестации и оценочные материалы

3.1. Входной контроль

Форма: тестирование

Описание, требования к выполнению: слушателям предлагается тест из 10 вопросов.

Критерии оценивания: тест считается выполненным, если слушатели выполнили более 70% заданий

Примеры заданий:

Вопрос 1: Инструменты работы в государственных информационных системах – это:

Варианты ответа:

А) Законченный последовательный набор команд, операторов, реализующих решение функциональной задачи.

Б) Набор цифровых сервисов и программных средств, которые обеспечивают взаимодействие участников образовательного процесса, управление данными и предоставление электронных услуг.

В) Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Г) Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Вопрос 2: К инструментам работы в государственных информационных системах в сфере образования не относятся:

Варианты ответа:

А) Инструменты для работы с данными и учёта.

Б) Инструменты для организации учебного процесса.

В) Инструменты для коммуникации и взаимодействия.

Г) Инструменты технического и программного управления рабочим местом.

Вопрос 3: К обязанностям поставщиков государственных информационных систем в сфере образования относится:

Варианты ответа:

А) Обеспечение своевременности, полноты и достоверности размещения, внесения информации в информационные системы;

Б) Соблюдение режимов обработки и использования информации, в том числе персональных данных;

В) Использование информационных систем в соответствии с целями и задачами их создания;

Г) Всё вышеперечисленное.

Количество попыток: не ограничено

3.2. Промежуточный контроль

Раздел программы: 4.2 Организация проведения оценки соответствия требованиям безопасности, предъявляемым к автоматизированным рабочим местам, подключенным к государственным информационным системам в сфере образования

Практическая работа № 1: проведение аудита защищенности информации, обрабатываемой на автоматизированном рабочем месте.

Описание, требования к выполнению:

Проведение слушателем аудита защищенности информации, обрабатываемой на автоматизированном рабочем месте организации, в целях подключения рабочего места к РГИС ЕРИСО КО.

Шаги выполнения:

1. В личном кабинете курса выберете один из двух способов подключения рабочего места к РГИС ЕРИСО КО.

с помощью защищенной сети ViPNet;

с помощью виртуальных сетей TLS на базе КриптоПРО.

2. В соответствии с выбранным способом скачайте шаблон Протокола оценки соответствия АРМ пользователя РГИС ЕРИСО КО требованиям безопасности информации.

3. Произведите аудит принятых в Вашей организации организационных, режимных и технических мероприятий информационной безопасности в соответствии с пунктами Протокола оценки соответствия. Заполните шаблон Протокола.

Результат выполнения: заполненный Протокол оценки соответствия автоматизированного рабочего места пользователя РГИС ЕРИСО КО требованиям безопасности информации.

Критерии оценивания:

Оформление согласно требованиям нормативных документов (0-2 балла).
Соблюдение структуры шаблонов документов (0-2 балла).
Полнота составленного комплекта документов (0-2 балла).
Качество составленного комплекта документов (0-2 балла).
Отражение актуальных сведений о принятых мерах защиты информации (0-2 балла).

Максимальная оценка – 10 баллов.
Минимальная оценка для зачета – 6 баллов.

Количество попыток: не ограничено.

3.3. Итоговая аттестация

Форма: тестирование

Описание, требования к выполнению: слушателям предлагается тест из 20 вопросов

Критерии оценивания: тест считается выполненным, если слушатели выполнили более 70% заданий

Примеры заданий:

Вопрос 1: Назначение приказом руководителя организации ответственных лиц за работу на автоматизированных рабочих местах относится к:

Варианты ответа:

А) Организационным мероприятиям информационной безопасности

Б) Физическим мероприятиям информационной безопасности

В) Техническим мероприятиям информационной безопасности

Г) Не относится к мероприятиям безопасности

Вопрос 2: Регистрация действий пользователей (событий) является:

Варианты ответа:

А) Функцией СЗИ от утечки информации по техническим каналам

Б) Функцией СЗИ от специальных воздействий

В) Функцией СЗИ от несанкционированного доступа к информации

Г) Функцией средств криптографической защиты информации

Вопрос 3: Шифрование информации осуществляется:

Варианты ответа:

А) Программными средствами защиты информации

Б) Специальными средствами защиты информации

В) Программно-техническими средствами информации

Г) Средствами криптографической защиты информации

Количество попыток: 3.

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Организационно-методическое и информационное обеспечение программы

Нормативные документы

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

3) Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

5) Постановление Правительства РФ от 01.04.2025 № 411 «О государственной информационной системе профилактики безнадзорности и правонарушений несовершеннолетних».

6) Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

7) Приказ Федеральной службы безопасности Российской Федерации от 22.08.2026 № 321 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5-1 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" с использованием шифровальных (криптографических) средств».

8) Методический документ ФСТЭК России от 12 апреля 2026 г. Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах.

9) Методический документ ФСТЭК России от 25 декабря 2022 г. Рекомендации по безопасной настройке операционных систем Linux.

10) ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

11) Распоряжение министерства образования Кировской области от 26.08.2026 № 1039 «Об обеспечении защищенного доступа к ресурсам региональной государственной информационной системы «Единая региональная информационная система образования Кировской области» с использованием защищенной сети ViPNet № 25176».

12) Распоряжение министерства образования Кировской области от 21.09.2026 № 1138 «Об обеспечении защищенного доступа к ресурсам региональной государственной информационной системы «Единая региональная информационная система образования Кировской области» с использованием технологии виртуальных сетей TLS сервер КриптоПро NGate и СКЗИ КриптоПро CSP».

Основная литература

1. ViPNet Client 5 for Linux. Руководство пользователя, 2025. 81 с. URL: https://infotecs.ru/downloads/documents/vipnet-client-5/?ysclid=mvf5k8f9fb981736093 (дата обращения 18.10.2026).
2. ViPNet Client 5 for Linux. Руководство администратора, 2025. 128 с. URL: https://infotecs.ru/downloads/documents/vipnet-client-5/?ysclid=mvf5k8f9fb981736093 (дата обращения 18.10.2026).
3. Kaspersky Endpoint Security. Подготовительные процедуры и руководство по эксплуатации, 2026. 492 с. URL: https://clck.su/fnAi (дата обращения 17.10.2026).
4. ViPNet EndPoint Protection for Linux Руководство администратора, 2026. 272 с. URL: https://infotecs.ru/products/vipnet-endpoint-protection/?tab=materials (дата обращения 18.10.2026).
5. ViPNet EndPoint Protection. Руководство пользователя, 2026. 26 с. URL: https://infotecs.ru/products/vipnet-endpoint-protection/?tab=materials (дата обращения 17.10.2026).
6. Операционная система специального назначения «Astra linux special edition». Руководство администратора. Часть 1. РУСБ.10015-01 95 01-1, 2024. 389 с. URL: https://clck.su/zeIMn (дата обращения 17.10.2026).
7. Операционная система специального назначения «Astra linux special edition». Руководство пользователя, 2024. 15 с. URL: https://clck.su/zGXGC (дата обращения 17.10.2026).
8. Альт Рабочая станция 11.2. Руководство пользователя, 2026 [Электронный ресурс]. URL: https://docs.altlinux.org/ru-RU/alt-workstation/11.2/html/alt-workstation/index.html.
9. Администрирование ОС Альт 11. Руководство администратора, 2026[Электронный ресурс]. URL: https://docs.altlinux.org/ru-RU/alt-admin/11.1/html-single/alt-admin/index.html

4.2. Материально-технические условия реализации программы

Технические средства обучения

Перечень необходимых технических средств обучения, используемых в учебном процессе для освоения программы повышения квалификации:

- информационная среда платформы дистанционного обучения КОГОАУ ДПО «ИРО Кировской области» https://edu.kirovipk.ru/;
- стационарные компьютеры, ноутбуки, проектор, экран;
- программы для подготовки и просмотра текстовых документов, электронных таблиц, компьютерных презентаций, цифровых видео, файлов с расширением pdf, jpeg, jpg;
- колонки, камера, микрофон (для осуществления онлайн консультирования обучающихся, при необходимости);
- возможность выхода в сеть Интернет для работы в системе дистанционного обучения, использования материалов, размещенных на внешних информационных ресурсах, возможность использования облачных технологий.