

**Кировское областное государственное образовательное автономное
учреждение дополнительного профессионального образования
«Институт развития образования Кировской области»
(КОГОАУ ДПО «ИРО Кировской области»)**

ПРИНЯТО:

Решение Ученого Совета

№ 8

«20» сентября 2023

ПТВЕРЖДАЮ:

Ректор

Н.В. Соколова

2023



ПОЛОЖЕНИЕ

**об отделе информационной безопасности
Центра цифровой трансформации системы образования
Кировской области
КОГОАУ ДПО «ИРО Кировской области»**

Киров
2023

1. Общие положения

1.1. Настоящее Положение об отделе информационной безопасности Центра цифровой трансформации системы образования Кировской области (далее – Положение) определяет правовой статус, цели, задачи, функции, права, взаимодействие, ответственность отдела информационной безопасности Центра цифровой трансформации системы образования Кировской области (далее – отдел).

1.2. Отдел является структурным подразделением Кировского областного государственного образовательного автономного учреждения дополнительного профессионального образования «Институт развития образования Кировской области» (КОГОАУ ДПО «ИРО Кировской области») (далее – Институт), входит в состав Центра цифровой трансформации системы образования Кировской области (далее – Центр).

1.3. Отдел создан с целью администрирования и сопровождения системы защиты информации в региональной государственной информационной системе «Единая региональная информационная система образования Кировской области» (далее – РГИС ЕРИСО) в соответствии с требованиями законодательства Российской Федерации, предъявляемыми к государственным информационным системам и к информационным системам персональных данных.

1.4. Отдел в своей деятельности руководствуется Конституцией Российской Федерации, федеральным законодательством, регламентирующим деятельность в сфере защиты информации, руководящими актами Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Уставом Института, настоящим Положением и иными локальными нормативными актами Института.

1.5. Отдел непосредственно подчиняется директору Центра, деятельность отдела курируется проректором по цифровому развитию.

1.6. Штатное расписание отдела определяется ректором Института по представлению проректора по цифровому развитию, исходя из потребности обеспечения функций отдела, обозначенных директором Центра.

1.7. Права, обязанности и ответственность работников отдела регламентируются трудовыми договорами и должностными инструкциями, утвержденными в установленном порядке.

1.8. Работа отдела организуется на основе текущего планирования, персональной ответственности каждого работника отдела за состояние дел на порученном участке работы и выполнение отдельных поручений.

1.9. Создание и упразднение отдела производится на основании решения Ученого совета Института по предварительному согласованию с учредителем Института.

1.10. Внесение изменений и дополнений в настоящее Положение производится на основании решения Ученого совета Института.

2. Цели и задачи отдела

2.1. Целями создания отдела являются:

2.1.1. Обеспечение защищенности информации от угроз информационной безопасности (в том числе нарушения конфиденциальности, целостности, доступности информации) при её обработке в РГИС ЕРИСО, а также при информационном обмене с внешними информационными системами.

2.1.2. Выполнение в РГИС ЕРИСО требований федерального законодательства, подзаконных нормативных правовых актов, руководящих документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности, регламентирующих вопросы защиты информации.

2.1.3. Поддержка функционирования и контроль соответствия аттестату соответствия требованиям безопасности средств и подсистем безопасности РГИС ЕРИСО.

2.1.4. Защищенная связь с федеральными и региональными государственными информационными системами, входящими в перечень информационных ресурсов, с которыми министерством образования Кировской области организовано защищенное межсетевое взаимодействие посредством РГИС ЕРИСО.

2.2. Задачами отдела являются:

2.2.1. Планирование мероприятий по защите информации в РГИС ЕРИСО.

2.2.2. Анализ угроз безопасности информации в РГИС ЕРИСО.

2.2.3. Управление (администрирование) системой защиты информации РГИС ЕРИСО.

2.2.4. Управление конфигурацией РГИС ЕРИСО и ее системой защиты информации.

2.2.5. Реагирование на инциденты РГИС ЕРИСО.

2.2.6. Информирование и обучение персонала РГИС ЕРИСО.

2.2.7. Контроль за обеспечением уровня защищенности информации, содержащейся в РГИС ЕРИСО.

2.2.8. Обеспечение информационной безопасности систем и сервисов Института.

2.2.9. Обеспечение конфиденциальности персональных данных и информации, обрабатываемой в РИС ЕРИСО.

3. Функции отдела

3.1. Планирование мероприятий по защите информации в РГИС ЕРИСО.

В ходе планирования мероприятий по защите информации в РГИС ЕРИСО осуществляются:

определение лиц, ответственных за планирование и контроль мероприятий по защите информации в РГИС ЕРИСО;

определение лиц, ответственных за выявление инцидентов и реагирование на них;

разработка, актуализация плана мероприятий по защите информации в РГИС ЕРИСО, направление плана мероприятий в министерство образования Кировской области в целях его утверждения;

определение порядка контроля выполнения мероприятий по обеспечению защиты информации в РГИС ЕРИСО, предусмотренных утвержденным планом.

3.2. Анализ угроз безопасности информации в РГИС ЕРИСО.

В ходе анализа угроз безопасности информации в РГИС ЕРИСО в ходе ее эксплуатации осуществляются:

выявление, анализ и устранение уязвимостей РГИС ЕРИСО;

анализ изменения угроз безопасности информации в РГИС ЕРИСО;

оценка возможных последствий реализации угроз безопасности информации в РГИС ЕРИСО.

3.3. Управление (администрирование) системой защиты информации РГИС ЕРИСО.

В ходе управления (администрирования) системой защиты информации РГИС ЕРИСО осуществляются:

определение лиц, ответственных за управление (администрирование) системой защиты информации РГИС ЕРИСО;

управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в РГИС ЕРИСО;

управление средствами защиты информации РГИС ЕРИСО;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования РГИС ЕРИСО;

централизованное управление системой защиты информации РГИС ЕРИСО;

мониторинг и анализ зарегистрированных событий в РГИС ЕРИСО, связанных с обеспечением безопасности (далее – события безопасности);

обеспечение функционирования системы защиты информации РГИС ЕРИСО в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

3.4. Управление конфигурацией РГИС ЕРИСО и ее системой защиты информации.

В ходе управления конфигурацией РГИС ЕРИСО и ее системы защиты информации осуществляются:

определение лиц, которым разрешены действия по внесению изменений в конфигурацию РГИС ЕРИСО и ее системы защиты информации, и их полномочий;

определение компонентов РГИС ЕРИСО и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

управление изменениями РГИС ЕРИСО и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в РГИС ЕРИСО и ее систему защиты информации, документирование

действий по внесению изменений в РГИС ЕРИСО и сохранение данных об изменениях конфигурации;

контроль действий по внесению изменений в РГИС ЕРИСО и ее систему защиты информации.

3.5. Реагирование на инциденты РГИС ЕРИСО.

В ходе реагирования на инциденты осуществляются:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в РГИС ЕРИСО;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению РГИС ЕРИСО и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3.6. Информирование и обучение персонала РГИС ЕРИСО.

В ходе информирования и обучения персонала РГИС ЕРИСО осуществляются:

информирование персонала РГИС ЕРИСО об угрозах безопасности информации, о правилах безопасной эксплуатации РГИС ЕРИСО;

доведение до персонала РГИС ЕРИСО требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

обучение персонала РГИС ЕРИСО правилам эксплуатации отдельных средств защиты информации;

проведение практических занятий и тренировок с персоналом РГИС ЕРИСО по блокированию угроз безопасности информации и реагированию на инциденты;

контроль осведомленности персонала РГИС ЕРИСО об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

3.7. Контроль за обеспечением уровня защищенности информации, содержащейся в РГИС ЕРИСО.

В ходе контроля за обеспечением уровня защищенности информации, содержащейся в РГИС ЕРИСО, осуществляются:

контроль (анализ) защищенности информации с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации;

анализ и оценка функционирования РГИС ЕРИСО и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации РГИС ЕРИСО;

документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в РГИС ЕРИСО;

доведение до министерства образования Кировской области информации о необходимости доработки (модернизации) системы защиты информации РГИС ЕРИСО.

3.8. Обеспечение информационной безопасности Института.

В ходе обеспечения информационной безопасности Института осуществляются:

сопровождение информационных систем Института, в том числе и обеспечение информационной безопасности серверов;

обеспечение защиты персональных данных в информационных системах Института;

обслуживание средств и систем защиты информации, включая средства криптографической защиты информации;

техническая поддержка системной инфраструктуры Института.

3.9. Обеспечение конфиденциальности персональных данных и информации, обрабатываемой в РИС ЕРИСО.

В рамках обеспечения конфиденциальности персональных данных и информации, обрабатываемой в РИС ЕРИСО осуществляется:

реализация безопасной обработки персональных данных и информации, обрабатываемой в РГИС ЕРИСО в соответствии с законодательством Российской Федерации и эксплуатационно-технической документацией;

использование информации, находящейся в РГИС ЕРИСО, исключительно в служебных целях, ее недоступность третьим лицам частично или полностью, за исключением случаев, предусмотренных законодательством Российской Федерации и Кировской области.

4. Права отдела

Отдел имеет следующие права:

4.1. Взаимодействовать с другими структурными подразделениями Института, органами управления, осуществляющими полномочия в сфере образования, а также другими организациями, по вопросам, входящим в компетенцию отдела и Центра.

4.2. Получать от министерства образования Кировской области, ректора и структурных подразделений Института информацию и другие материалы, необходимые для осуществления функций отдела и Центра.

4.3. Вносить предложения в министерство образования Кировской области об улучшении работы по организации защиты информации в РГИС ЕРИСО.

4.4. Создавать рабочие группы по вопросам, входящим в компетенцию отдела.

4.5. Разрабатывать методические материалы и рекомендации по вопросам, входящим в компетенцию отдела.

4.6. Знакомится с проектами решений руководящих органов Института, касающихся деятельности отдела, участвовать в их подготовке и обсуждении.

4.7. Вносить предложения ректору об улучшении работы по организации защиты информации в Институте.

4.8. Обращаться к руководству Института за содействием для исполнения функциональных обязанностей отдела.

5. Управление отделом

5.1. Руководство деятельностью отдела возлагается на начальника отдела, который назначается на должность и освобождается с должности приказом ректора Института.

5.2. Обязанности начальника отдела определяются должностной инструкцией и в каждом отдельном случае заключенным трудовым договором с учетом специфики отдела и Центра.

5.3. Начальник отдела в своей деятельности руководствуется действующим законодательством РФ, локальными нормативными актами Института, настоящим Положением, должностной инструкцией.

5.4. Начальник отдела в своей деятельности подчиняется директору Центра.

5.5. В период отсутствия начальника отдела (командировка, отпуск, болезнь и т.д.) его обязанности исполняет работник, назначенный в установленном порядке, который приобретает соответствующие права и несет ответственность за неисполнение или ненадлежащее исполнение обязанностей, возложенных на него в связи с замещением.

5.6. В пределах своих полномочий начальник отдела дает поручения, обязательные для исполнения всеми сотрудниками отдела.

5.7. Деятельность отдела осуществляется согласно перспективным и текущим планам работы, интегрированным в план-отчет Центра, утверждаемый на календарный год ректором Института или соответствующим проректором и скоординированным с планами работы Института, других структурных подразделений.

5.8. Отдел регулярно, согласно планам работы, участвует в заседаниях Центра (не реже 1 раза в месяц). Могут проводиться заседания отдельных рабочих групп, секций, а также совместные заседания с другими структурными подразделениями.

5.9. Отдел может проводить научные, научно-практические и методические конференции по проблемам обеспечения информационной безопасности образования, а также семинары, выставки и другие организационно-педагогические и научные мероприятия.

5.10. Вопросы, выносимые отделом на заседания Центра, определяются функциями, планами работы отдела и Центра, текущим положением и перспективами развития Института, системы дополнительного профессионального образования. По рассмотренным вопросам принимаются соответствующие решения.

5.11. Начальник отдела:

руководит деятельностью отдела и несет персональную ответственность за организацию и результаты выполнения возложенных на отдел задач и

функций, исполнения плана работы отдела и плана работы Института, в части касающейся отдела;

представляет по поручению ректора интересы Института в органах государственной власти, органах местного самоуправления, общественных объединениях при рассмотрении вопросов, относящихся к компетенции отдела;

распределяет должностные обязанности между работниками отдела; обеспечивает разработку должностных инструкций работников отдела; осуществляет отбор и расстановку кадров отдела и обеспечивает соблюдение работниками отдела исполнительской и трудовой дисциплины;

вносит руководству Института в соответствии с установленным порядком предложения об изменении структуры и штатного расписания отдела, о приеме на работу, назначении на должность и освобождении от должности, переводе, увольнении работников отдела, поощрении и применении мер дисциплинарного воздействия;

создает условия для повышения, улучшения условий труда работников отдела, внедрения передовых методов работы;

обеспечивает взаимодействие с другими структурными подразделениями Института по вопросам, отнесенным к компетенции отдела;

готовит в пределах своей компетенции предложения, подписывает и визирует документы, связанные с деятельностью отдела.

6. Взаимодействие отдела с другими подразделениями

Отдел взаимодействует:

6.1. со структурными подразделениями Института по вопросам наполнения контента информационных ресурсов, организации, подготовки и проведения курсов и мероприятий Института в рамках компетенции отдела;

6.2. со структурными подразделениями, реализующими учебную деятельность, при организации совместной работы по проектированию, разработке, экспертизе и сопровождению онлайн-курсов и электронных образовательных ресурсов в рамках компетенции отдела;

6.3. с начальником административно-хозяйственного отдела по вопросам обеспечения материальной базы отдела;

6.4. с финансово-экономическим отделом по своевременному оформлению документов на оплату;

6.5. с кадрово-юридическим отделом по вопросам кадрового обеспечения отдела, учета рабочего времени сотрудников и т.п.;

6.6. с другими структурными подразделениями Института по вопросам, относящимся к компетенции отдела.

7. Учет и отчетность

7.1. Делопроизводство в отделе ведется в соответствии с инструкцией по делопроизводству и номенклатурой дел Института.

8. Ответственность

8.1. Отдел несет ответственность за несвоевременное или некачественное исполнение возложенных на него функций и задач, за причинение материального ущерба, за разглашение служебной, коммерческой, персональной информации в соответствии с действующим законодательством РФ.