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

УТВЕРЖДАЮ:
И.о. ректора
_____ О.В. Казаринова
«__» _____ 2024

ПОРЯДОК

проведения периодических проверок (аудитов) в области обработки и обеспечения безопасности персональных данных в КОГОАУ ДПО «ИРО Кировской области»

Киров
2024

1. Общие положения

1.1. Назначение

Настоящий Документ определяет порядок организации и проведения внутренних проверок (аудитов) процессов обработки персональных данных (далее – Порядок) в Кировском областном государственном образовательном автономном учреждении дополнительного профессионального образования «Институт развития образования Кировской области» (далее – Институт).

1.2. Цель принятия документа

Настоящий Порядок принят в целях:

обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

своевременного обнаружения несоответствий требованиям процесса обработки персональных данных и их устранения.

1.3. Область применения

Настоящий документ применяется:

к процессам Института, в которых ведется обработка персональных данных;

ко всем структурным подразделениям Института.

1.4. Аудитория

Порядок предназначен для следующих категорий сотрудников Института и лиц:

сотрудник, ответственный за организацию обработки персональных данных;

сотрудники, в обязанности которых входит обработка персональных данных;

руководители подразделений;

сотрудники, в обязанности которых входит организация и обеспечение документооборота;

подразделения, в обязанности которых входит разработка и поддержка сервисов и информационных систем персональных данных;

лица, которым Институтом поручено обрабатывать персональные данные.

Под сотрудниками в настоящем положении понимаются лица, состоящие в трудовых или договорных отношениях с Институтом, а также сотрудники организаций, которым Институтом поручена обработка персональных данных (далее – «сотрудники»).

Перечисленные сотрудники перед предоставлением доступа к персональным данным должны быть ознакомлены с настоящим документом в соответствии с *Порядком предоставления доступа к персональным данным*.

1.5. Нормативные ссылки

Положение разработано в целях реализации следующих нормативно-правовых актов:

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

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

Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.6. Срок действия и порядок внесения изменений

Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Порядок подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, требований со стороны контрагентов, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путем издания новой версии и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

Срок хранения после прекращения действия: постоянно.

1.7. Используемые сокращения

СКЗИ – средства криптографической защиты информации.

2. Порядок проведения проверок

2.1. Общие сведения о внутренних проверках (аудитах)

Внутренние проверки (аудиты) проводятся с целью оценки соответствия требованиям процессов обработки персональных данных в Институте.

Внутренние проверки (аудиты) соответствия принимаемых мер по обеспечению безопасности персональных данных и установленного уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных, должны проводиться не реже 1 раза в 3 года. Для проведения таких проверок (аудитов) могут привлекаться на основании договора подрядные организации, имеющие лицензию Федеральной службы по техническому и экспортному контролю Российской Федерации на деятельность по технической защите конфиденциальной информации, а также, при необходимости, лицензию Федеральной службы безопасности Российской Федерации на деятельность, связанную со средствами шифрования.

Организация аудитов включает:

Разработку программы внутренних проверок (аудитов);

Разработку плана внутренних проверок (аудитов);

Проведение внутренних проверок (аудитов).

Программа проверок (аудитов) – совокупность мероприятий по проведению одной или нескольких проверок (аудитов), запланированных на конкретный период времени и направленных на достижение конкретной цели

– обеспечение соответствия процессов обработки персональных данных требованиям законодательства, нормативных документов и документов, принятых в Институте.

План проверки (аудита) - описание деятельности и мероприятий по проведению проверки (аудита).

2.2. Порядок формирования программы проверок (аудитов)

Программа проверок (аудитов) планируется сроком на 1 календарный год.

При проведении проверок (аудитов) необходимо учитывать степень доступности сотрудников, задействованных в их проведении.

В отсутствие ресурсов для выполнения программы проверок (аудитов) может быть приглашен внешний аудитор.

Программа проверок (аудитов) должна быть составлена таким образом, чтобы за проверяемый период были охвачены:

все процессы обработки персональных данных;

все подразделения;

все географические расположения;

все сервисы и информационные системы Института.

Типовая форма программы внутренних проверок (аудитов) приведена в Приложении № 1.

2.3. План проверки (аудита)

План внутренней проверки (аудита) процессов обработки и обеспечения безопасности персональных данных формируется сотрудником, ответственным за проведение проверки (аудита) – внутренним аудитором и согласовывается с сотрудником, ответственным за организацию обработки персональных данных и сотрудником, ответственным за обеспечение безопасности персональных данных (информационной безопасности) в Институте.

Перечень и описание отдельных вариантов проверок, которые должны быть включены в план, приведен в разделе 3 Порядка.

План должен включать:

– Сроки проведения проверки;

– Подразделение, в котором проходит проверка;

– Наименование мероприятия, входящего в проверку (раздел 3 Порядка);

– Формы проверки (очная, заочная, по документам, с интервьюированием);

– Ответственный за проведение проверки (аудиторская комиссия).

В зависимости от структуры подразделений, особенностей процессов и разграничения полномочий план проверки (аудита) может быть разработан специально под отдельное подразделение или пли процесс.

2.4. Порядок оповещения работников о проведении проверки

Работники Института должны быть оповещены о проведении проверки не позднее, чем за 5 рабочих дней до её начала. Оповещение должно содержать план проверки.

2.5. Отчет о результатах проверки (аудита)

По итогам проверки (аудита) внутренним аудитором (комиссией аудиторов) формируется отчет, представляющий собой совокупность наблюдений о соответствии или несоответствии требованиям проверенных подразделений и процессов.

Наблюдения фиксируются в электронной таблице в виде записей, содержащих:

1) Наименование мероприятия из программы внутренних проверок;
2) Подразделение, в котором проводилась проверка;
3) Нормативное требование (пункт федерального закона, иного нормативного документа или локального акта);
4) Соответствие/несоответствие требованиям;
5) Описание выявленных нарушений;
6) Сотрудник, ответственный за устранение несоответствия;
7) Срок устранения нарушения.

2.5.3. Таблица после составления распечатывается и подписывается аудитором (комиссией аудиторов).

Сотрудник, ответственный за организацию обработки персональных данных, обеспечивает ведение реестра несоответствий и нарушений, организовывает работу по их устранению, координирует и содействует работе ответственных за устранение несоответствий и нарушений.

При выявлении совокупности одинаковых несоответствий, либо в случае выявления отдельного практически-сложного случая, может потребоваться создание рабочей группы наблюдения или выделение дополнительных ресурсов. Такая группа наблюдений или кейс формируются в проект и выполняются в форме проекта, включая обоснование, формирование технического задания, выполнение работ, закупку, принятие в эксплуатацию. Лицами, обеспечивающими реализацию таких проектов в Институте являются *сотрудник ответственный за организацию обработки персональных данных* и *сотрудник ответственный за безопасность персональных данных (информационную безопасность)*.

3. Перечень мероприятий, проводимых в рамках проверок

3.1. Проверка соблюдения принципов обработки персональных данных

В ходе проверки соблюдения принципов обработки персональных данных осуществляются следующие мероприятия:

проверка актуальности документов, определяющих политику Института в отношении обработки персональных данных;

проверка процессов обработки персональных данных на предмет обработки избыточных персональных данных, а также на предмет превышения установленных сроков хранения персональных данных;

проверка обоснованности установленных целей обработки персональных данных.

3.2. Проверка правовых оснований для обработки персональных данных

В ходе проверки правовых оснований для обработки персональных данных осуществляются мероприятия:

проверка договоров с субъектами персональных данных;

проверка договоров с лицами, которым Институтом поручена обработка персональных данных;

проверка договоров с лицами, которые поручают Институту обработку персональных данных;

проверка наличия согласий в ситуациях, когда такое основание необходимо;

проверка наличия согласий в письменной форме, если такие согласия необходимы;

проверка наличия законных и иных оснований для обработки персональных данных;

проверка сроков обработки персональных данных и наличия правовых оснований.

3.3. Проверка соблюдения Порядка предоставления доступа к обработке персональных данных

В ходе проверки соблюдения *Порядка предоставления допуска к персональным данным* осуществляются следующие мероприятия:

проверка актуальности документа *«Перечень должностей сотрудников, допущенных к обработке персональных данных в автоматизированной форме и без использования средств автоматизации»*;

проверка наличия заполненных листов (журналов) ознакомления сотрудника под роспись с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Института в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

проверка ведения *журнала инструктажей по правилам обработки и обеспечения безопасности персональных данных*;

проверка наличия подписанных *обязательств о неразглашении конфиденциальной информации*;

проверка наличия заявок на предоставление (изменение/прекращение) доступа к информационным системам персональных данных;

проверка наличия учетных записей пользователей;

проверка соответствия прав доступа пользователей в информационных системах персональных данных ранее поданным заявкам на предоставление доступа.

3.4. Проверка соблюдения порядка взаимодействия с субъектами персональных данных

В ходе проверки соблюдения *Положения о порядке взаимодействия с субъектами персональных данных и их представителями по вопросам обработки персональных данных* осуществляются следующие мероприятия:

проверка порядка принятия и обработки обращений и вопросов субъектов персональных данных;

проверка времени реагирования на обращения субъектов персональных данных согласно требованиям ст.14, 20, 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

проверка факта размещения политики обработки персональных данных в открытом доступе;

проверка ведения журнала учета обращений субъектов;

проверка осведомленности работников о порядке взаимодействия с субъектами персональных данных, в том числе о правах субъектов персональных данных;

проверка осведомленности сотрудников по вопросам разъяснения юридических последствий отказа субъекта в предоставлении персональных данных.

3.5. Проверка порядка обращения с машинными носителями персональных данных

В ходе проверки порядка обращения с машинными носителями персональных данных осуществляются следующие мероприятия:

проверка ведения *Журнала учета съемных носителей*;

проверка условий хранения съемных носителей, выданных работникам;

проверка ведения *Журнала учета несъемных машинных носителей*;

проверка порядка уничтожения машинных носителей персональных данных, в т.ч. наличие *Актов уничтожения*;

проверка осведомленности работников о порядке использования съемных машинных носителей персональных данных.

3.6. Проверка соблюдения Порядка неавтоматизированной обработки персональных данных

В ходе проверки соблюдения *Инструкции по обработке персональных данных, осуществляемой без использования средств автоматизации* осуществляются следующие мероприятия:

проверка актуальности и соблюдения сотрудниками документа *«Перечень мест хранения материальных носителей персональных данных*;

проверка сохранности бумажных носителей персональных данных;

проверка осведомленности работников о порядке неавтоматизированной обработки персональных данных;

проверка избыточности хранения документов;

проверка типовых форм документов, с использованием которых ведется сбор персональных данных;

проверка актов уничтожения документов.

3.7. Проверка условий эксплуатации средств криптографической защиты информации

В ходе проверки условий эксплуатации средств криптографической защиты информации (далее – СКЗИ) осуществляются следующие мероприятия:

проверка оснащения серверных помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии (либо проверка опечатывания серверных помещений);

проверка актуальности утвержденного перечня лиц, имеющих право доступа в серверные помещения;

проверка назначения администратора СКЗИ, пользователей СКЗИ;

проверка наличия и порядка хранения инструкции по эксплуатации СКЗИ, инструкции пользователя СКЗИ, дистрибутивов СКЗИ, формуляра СКЗИ;

проверка соблюдения требований инструкции по эксплуатации СКЗИ, правил пользования СКЗИ.

Приложение № 1. Типовая форма плана внутренних проверок

План
внутренних проверок (аудитов) процессов обработки
и обеспечения безопасности персональных данных

_____
(период)

Сроки проведения	Подразделение	Наименование мероприятия	Формы проверки	Ответственный за проведение
с (__.__.___) по (__.__.___)	Наименование структурного подразделения	Проверка соблюдения принципов обработки персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка предоставления доступа к обработке персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка правовых оснований для обработки персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка взаимодействия с субъектами персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка порядка обращения с машинными носителями персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка порядка эксплуатации персональных компьютеров при доступе к сервисам и информационным системам персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка соблюдения порядка неавтоматизированной обработки персональных данных		*(Фамилия И.О.)*
с (__.__.___) по (__.__.___)		Проверка условий эксплуатации средств криптографической защиты информации		*(Фамилия И.О.)*
с (__.__.___)		Подготовка ежегодного отчета по результатам внутренних проверок		*(Фамилия И.О.)*

Сроки проведения	Подразделение	Наименование мероприятия	Формы проверки	Ответственный за проведение
по (__.__.___)		порядка обработки и обеспечения безопасности персональных данных		

УТВЕРЖДАЮ

_____
(должность)

_____ / _____

«____» _____ 20___ г.
(форма)

ОТЧЕТ
по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
в _____
(наименование организации)

Настоящее заключение составлено о том, что в период с «___» _____ 20__ г. по «___» _____ 20__ г. Комиссией _____
_____(далее – Организация) в составе:
(наименование организации)
_____
_____
_____
_____

проведена проверка соответствия обработки персональных данных в Организации требованиям федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Организации в отношении обработки персональных данных, локальным актам Организации
(тема проверки, подразделение)

Проверка осуществлялась в соответствии с требованиями:
1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
2. Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
4. Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
(название документа)

В ходе проверки проверены:
помещения Организации, в которых осуществляется обработка персональных данных:
_____
_____
_____
_____
(перечислить помещения, в которых проводилась проверка)

В ходе проверки установлено:

Наименование мероприятия из программы внутренних проверок	**Подразделение, в котором проводилась проверка**	**Нормативное требование (пункт федерального закона, иного нормативного документа или локального акта)**	**Соответствие/ несоответствие /рекомендация**	**Описание нарушений**	**Сотрудник, ответственный за устранение несоответствия**	**Срок устранения нарушения**

Председатель комиссии:

_____/ _____ / _____
фамилия и инициалы / подпись / должность

Члены комиссии:

_____/ _____ / _____
фамилия и инициалы / подпись / должность

_____/ _____ / _____
фамилия и инициалы / подпись / должность