Приложение № 5
к приказу от «29» 12 2021 г. № 57
«Об организации работ по
защите персональных данных по требованиям
информационной безопасности»

«О порядке обработки персональных данных субъектов Частного образовательного учреждения дополнительного профессионального образования «Корпоративный институт энергетики»

ИНСТРУКЦИЯ
об осуществлении контроля выполнения требований по защите персональных данных в
Частного образовательного учреждения дополнительного профессионального образования «Корпоративный институт энергетики»

Настоящая инструкция определяет порядок организации и осуществления контроля выполнения требований по защите персональных данных в структурных подразделениях Частного образовательного учреждения дополнительного профессионального образования «Корпоративный институт энергетики» (далее – Учреждение).

Требования инструкции обязательны для исполнения всеми должностными лицами Учреждения, осуществляющими контроль состояния защиты персональных данных.

1. Общие положения

Контроль выполнения требований по защите персональных данных в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет Ответственный за организацию обработки персональных данных Учреждения. Для участия в проведении контроля решением Ответственного за организацию обработки персональных данных могут также привлекаться другие специалисты подразделений Учреждения (по согласованию с их руководителями). В таких случаях контроль носит комплексный характер.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Учреждения или нарушения требований по защите персональных данных.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала

проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений.

Периодичность и сроки проведения плановых проверок подразделений Учреждения устанавливаются графиком проверок на календарный год. План утверждает Директор Учреждения. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа Директора Учреждения. Осуществляет проверку комиссия или группа лиц из состава сотрудников Учреждения. Состав комиссии или группы лиц определяется приказом Директора Учреждения о проверке.

Ответственный за организацию обработки персональных данных Учреждения подготавливает предложения по составу комиссии или группы проверяющих лиц. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных Учреждения.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в подразделение для проведения проверки председатель комиссии (старший по проверке) прибывает к руководителю проверяемого подразделения Учреждения, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение

проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления сотрудников проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии сотрудников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких должностных лиц подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по защите персональных данных в подразделении Учреждения рассматриваются в частности следующие показатели:

1) в части общей организации работ по защите персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

б) наличие нормативных документов по защите персональных данных;

в) знание нормативных документов сотрудниками, имеющими доступ к персональным данным;

г) полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к персональным данным;

д) наличие документов, определяющих состав сотрудников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

е) уровень подготовки сотрудников, ответственных за организацию защиты персональных данных в подразделении;

ж) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учета носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего

учета носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность классификации информационной системы;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о подразделениях Учреждения, должностных инструкциях сотрудников и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учета, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт (служебная записка) составляется в двух экземплярах и подписывается членами комиссии или группой проверяющих лиц. Один экземпляр хранится у ответственного за организацию обработки персональных данных Учреждения. Второй экземпляр хранится в Учреждении в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок подразделений периодически обобщаются ответственным за организацию обработки персональных данных Учреждения и доводятся до руководителей подразделений. При необходимости принятия решений по результатам проверок подразделений Директору Учреждения готовятся соответствующие служебные записки.

Информация о разработчике Положения

Дата разработки:	29.12.2021
Разработчик: Системный администратор	Азарня Вячеслав Эдикович
Телефон, e-mail:	8(8793)45-86-90 sisadmin@uk-skfo.ru

Прошито, пронумеровано и скреплено
печатью 7 (семь) лист

И.о. юрисконсульта
ЧОУ ДПО «Корпоративный институт энергетики»
_____ Е.С. Осьмакова
«29» 12 2021 г.