«СОГЛАСОВАНО»
Председатель профсоюзного комитета студентов и преподавателей
Усманского педагогического колледжа

_____ Н.Е. Глазкова
« 01 » 04 2022 г.

Петухов Сергей Григорьевич

Подписан: Петухов Сергей Григорьевич
DN: C=RU, OU=директор, O="ГОБПОУ ""Усманский многопрофильный колледж""", CN=Петухов Сергей Григорьевич, E=uspk@yandex.ru
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2023.01.11 16:05:29+03'00'

«Усманский многопрофильный колледж»
_____
Приказ № 36 от « 01 » 04 2022 г.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных работников и обучающихся Государственного областного бюджетного профессионального образовательного учреждения «Усманский многопрофильный колледж»

г. Усмань

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных работников и обучающихся (далее - Правила контроля) в ГОБПОУ «Усманский многопрофильный колледж» (далее – колледж, образовательное учреждение) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных работников и обучающихся (далее – ПД); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПД, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПД.

1.2. Настоящие Правила контроля разработаны в соответствии с:

- Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Перечнем мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утв. постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211;
- Уставом колледжа и иными ЛНА образовательного учреждения.

1.3. Колледж использует информационные системы персональных данных (далее - ИСПД) для выполнения основных целей и задач обработки ПД, указанных в Положении о защите, хранении, обработке и передаче персональных данных работников ГОБПОУ «Усманский многопрофильный колледж».

1.4. Пользователями ИСПД (далее - Пользователи) являются работники колледжа, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПД и имеющие доступ к аппаратным средствам, программному обеспечению (далее - ПО), данным и средствам защиты информации (далее - СЗИ) ИСПД.

1.5. Контрольные мероприятия по обеспечению уровня защищенности ПД и соблюдению условий использования СЗИ, а также соблюдению требований законодательства Российской Федерации по обработке ПД в ИСПД колледжа проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в колледже и действующего законодательства Российской Федерации в области обработки и защиты ПД;
- оценка уровня осведомленности и знаний сотрудников колледжа в области обработки и защиты ПД;
- оценка обоснованности и эффективности применяемых мер и средств защиты ПД.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПД требованиям к защите ПД:

2.1. Проверки соответствия обработки ПД установленным требованиям в колледже разделяются на следующие виды:

- регулярные;

- плановые;

- внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся администратором ИС (ответственное лицо) в соответствии с утвержденным планом (приложение 1 к настоящим Правилам) проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в колледже.

2.3. Плановые контрольные мероприятия периодически проводятся постоянной комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты ПД ИСПД колледжа.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;

- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

- по решению руководителя образовательного учреждения.

2.5. Ответственное лицо (администратор ИС) за проведение регулярных контрольных мероприятий; состав постоянной комиссии по проведению плановых контрольных мероприятий; состав комиссии по информационной безопасности на период проведения внеплановых контрольных мероприятий, - установлены Перечнем лиц, осуществляющих проведение контрольных мероприятий (приложение 2 к настоящим Правилам).

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает план внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;

- задачи проведения контрольных мероприятий;

- объекты контроля (процессы, подразделения, информационные системы и т.п.);

- состав участников, привлекаемых для проведения контрольных мероприятий;

- сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в журнале учета событий информационной безопасности (приложение 3 к настоящим Правилам).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий ответственное лицо или члены комиссии разрабатывают отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;

- перечень и описание выявленных нарушений;

- рекомендации по устранению выявленных нарушений;

- заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение руководителя колледжа.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в Протокол проведения внутренних проверок контроля соответствия обработки ПД требованиям к защите ПД в колледже (приложение 4 к настоящим Правилам).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПД.

Также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности ПД информационных систем ПД.

5.2. Лицо, ответственное за обеспечение безопасности ПД, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий в зависимости от целей мероприятий могут выполняться следующие проверки:

- соответствия полномочий Пользователя правилам доступа;

- соблюдения Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПД;

- соблюдения администраторами ИСПД инструкций и регламентов по обеспечению безопасности информации в колледже;

- соблюдения порядка доступа сотрудников в помещения образовательного учреждения, где ведется обработка персональных данных;

- знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций;

- знание администраторами ИСПД инструкций и регламентов по обеспечению безопасности информации в колледже;

- порядок и условия применения средств защиты информации;

- состояние учета машинных носителей ПД;

- наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер;

- проведенные мероприятия по восстановлению ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;

-технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты.

6. Заключительные положения

5.1. Настоящие Правила вступают в силу с «____» _____ 202__ г.

5.2. В данные правила могут вноситься изменения и дополнения, не противоречащие действующему законодательству РФ и Уставу колледжа.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия обработки
персональным данным требованиям к защите персональных данных

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Специалист по кадрам
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) межведомственного обмена	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Контроль обновления ПО и единообразия, применяемого ПО на всех элементах ИС	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия по проведению ПКМ
Поддержание в актуальном состоянии нормативно-организационных документов	Еженедельно	Ежемесячно	Специалист по кадрам
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Ответственное лицо и Комиссия

			по проведению ПКМ

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных

ПЕРЕЧЕНЬ
лиц, осуществляющих проведение контрольных мероприятий

1. Проведение регулярных контрольных мероприятий (ответственное лицо)

№ п/п	ФИО работника	Занимаемая должность	Подпись

2. Проведение плановых контрольных мероприятий

№ п/п	ФИО работника	Занимаемая должность	Подпись

3. Проведение внеплановых контрольных мероприятий

№ п/п	ФИО работника	Занимаемая должность	Подпись

Приложение 3
к Правилам осуществления внутреннего контроля соответствия обработки
персональным данным требованиям к защите персональных данных

ЖУРНАЛ
учета событий информационной безопасности
в ГОБПОУ «Усманский многопрофильный колледж»

Журнал начат
«____» _____ 202__ г.
Должность
_____
Подпись ответственного лица
_____

Журнал завершен
«____» _____ 202__ г.
Должность
_____
Подпись ответственного лица
_____

№ п/п	Дата события	Основания возникновения обстоятельств	Описание события (мероприятия)	Характеристика события	(ФИО субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приложение 4
к Правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен о том, что «_____» _____ 20___г.
проведена проверка

_____

_____

(должность, Ф.И.О. работника, обучающегося)

_____

_____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____

_____

(название документа)

В ходе проверки проверено:

_____

_____

_____

_____

Выявленные нарушения:

_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____

Срок устранения нарушений:

_____

Ответственное лицо:

_____

(фамилия и инициалы / подпись / должность)

Члены комиссии:

_____

_____

_____

(фамилия и инициалы / подпись / должность)