Приложение № 3
к приказу КФ МГГЭУ
от «30» июля 2021 г. № 95-п

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

КАЛМЫЦКИЙ ФИЛИАЛ

РАССМОТРЕНО
на педагогическом совете
Протокол № 01
«09» 09 2021 г.

УТВЕРЖДАЮ
Директор филиала
_____ Э.Л. Пашнанов
«09» 09 2021 г.

ПОЛОЖЕНИЕ
О ВНУТРЕННЕМ КОНТРОЛЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В
Калмыцком филиале федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет»

г. Элиста, 2021 г.

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле обработки и защиты персональных данных (далее - Положение) в Калмыцком филиале федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет» (далее - Филиал) определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля обработки и защиты ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Филиал использует информационные системы персональных данных (далее - ИСПДн) для выполнения основных целей и задач обработки ПДн.

1.3. Пользователями ИСПДн (далее - Пользователь) являются сотрудники Филиала, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющие доступ к аппаратным средствам, программному обеспечению (далее - ПО), данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.4. Контрольные мероприятия по обеспечению уровня защищенности ПДн и соблюдению условий использования СЗИ, а также соблюдению требований законодательства Российской Федерации по обработке ПДн в ИСПДн проводятся в следующих целях:

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

2. Тематика внутреннего контроля

Тематика внутреннего контроля обработки и защиты ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в Филиале разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся администратором ИС в соответствии с утвержденным планом проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в Филиале.

2.3. Плановые контрольные мероприятия периодически проводятся постоянной комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты ПДн ИСПДн Филиала.

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 директора филиала.

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 актах внутреннего контроля.

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 директора филиала.

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

5. Порядок проведения плановых и внеплановых контрольных мероприятий

Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности ПДн информационных систем ПДн.

5.1. Лицо, ответственное за обеспечение безопасности ПДн, 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.

5.2. 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 ПДн;
- соблюдения администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в Филиале;

- соблюдения порядка доступа сотрудников в помещения Филиала, где ведется обработка персональных данных;
- знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- знание администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в Филиале;
- порядок и условия применения средств защиты информации;
- состояние учета машинных носителей ПДн;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
- проведенные мероприятия по восстановлению ПДн, 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.

Приложение к Положению о
внутреннем контроле обработки и
защиты 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	Системный администратор
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Системный администратор
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Системный администратор
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Системный администратор
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Еженедельно	Ежемесячно	Системный администратор
Контроль обновления ПО и единообразия, применяемого ПО на всех элементах ИС	Еженедельно	Ежемесячно	Системный администратор
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Системный администратор
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Еженедельно	Ежегодно	Системный администратор
Поддержание в актуальном состоянии нормативно-организационных документов	Еженедельно	Ежемесячно	Специалист по кадрам
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Системный администратор

Приложение к Положению о внутреннем контроле обработки и защиты персональных данных

УТВЕРЖДАЮ

_____
(должность председателя комиссии)

_____ _____
(подпись) (расшифровка подписи)

Акт
"_____"_____20____г.
внутреннего контроля соответствия обработки персональных данных в структурных подразделениях _____

1. Результаты рассмотрения вопросов по предметам контроля:

Предмет контроля	**Результат рассмотрения**	**Примечание**
Документы, определяющие основания обработки персональных данных		
Утвержденные списки должностных лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей		
Утвержденные перечни информационных систем персональных данных		
Своевременность мероприятий по уничтожению либо обезличиванию персональных данных		
Условия хранения и состояние учета машинных носителей персональных данных		
Порядок и условия применения средств защиты информации при наличии таковых		
Соблюдение требований к паролям доступа		
Отсутствие неправомерно размещенных персональных данных граждан в разделах официального сайта		

2. Предложения комиссии:

_____

_____

Подписи членов комиссии:

_____ _____

(подпись) (фамилия, имя, отчество)

_____ _____

(подпись) (фамилия, имя, отчество)

_____ _____

(подпись) (фамилия, имя, отчество)