ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

РАССМОТРЕНО
на Совете филиала
Протокол № 01
«09» 09 2021 г.

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

ПОЛОЖЕНИЕ
О ВЫЯВЛЕНИИ, ЛИКВИДАЦИИ И ПРЕДОТВРАЩЕНИИ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ 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. Используемые термины и определения.

Информационная безопасность (далее - ИБ) - процесс обеспечения конфиденциальности, целостности и доступности информации.

Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие право доступа.

Целостность - избежание несанкционированной модификации информации.

Доступность - избежание временного или постоянного сокрытия информации от субъектов, получивших права доступа.

Защищаемая информация - в контексте настоящего Положения - персональные данные (далее - ПДн), обрабатываемые в Калмыцком филиале федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет» (далее – Филиал).

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Инцидент информационной безопасности - событие (серия, группа событий), указывающее на свершившуюся, предпринимаемую (попытка) или вероятную (предполагаемую) реализацию угрозы ИБ.

Угроза ИБ - нарушение процесса обеспечения доступности, целостности или конфиденциальности защищаемой информации.

1.2. Источники угроз ИБ:

- преднамеренные действия (со стороны внутреннего и/или внешнего нарушителя) в отношении носителей ПДн, средств обработки ПДн и среды их функционирования);
- непреднамеренные действия персонала (неумышленно допущенные, неквалифицированные действия, ошибки, случайные, нечаянные действия, действия по истинному заблуждению и т.п.);
- случайные факторы не антропогенного характера (ошибки и неисправности средств обработки ПДн, в т.ч. аппаратных комплексов, программного обеспечения, телекоммуникационных средств, связи и т.п.);
- природные факторы (пожар, наводнение, землетрясение и т.п.).

1.3. Объекты реализации угроз ИБ:

- носители информации, содержащей ПДн, в том числе материальные, машиночитаемые (отчуждаемые и встроенные в средства обработки ПДн) и т.п.;
- средства хранения носителей информации;
- средства обработки ПДн (автоматизированные, неавтоматизированные);
- среда функционирования средств обработки ПДн;
- места размещения средств обработки ПДН и хранилищ носителей информации;
- средства обеспечения безопасности (физической, защиты от несанкционированного доступа, криптографической и т.п.);
- среда функционирования средств обеспечения безопасности;
- документация различного рода, относящаяся к указанным выше объектам, от обеспечения безопасности которой, зависит вероятность предотвращения угроз ИБ.

1.4. Настоящее Положение обязательно к соблюдению всеми работниками Филиала (далее - работники), участвующими в выявлении, разбирательстве и предотвращении инцидентов ИБ.

2. Особенности организации выявления и предотвращения инцидентов ИБ

2.1. Ответственность за выявление инцидентов ИБ в информационной системе и реагирование на них в Калмыцком филиале федерального государственного бюджетного

образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет» возлагается на системного администратора.

2.2. Системный администратор имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед директором филиала) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

2.3. Системный администратор обязан вести журнал учёта инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

2.4. В журнале в свободной форме описывается инцидент с указанием следующих данных:

– даты и времени;

– причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;

– информации о последствиях.

2.5. Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

2.6. В случае возникновения рецидива со стороны пользователя или системного администратора, по ходатайству ответственного за организацию обработки персональных данных директором филиала накладывается дисциплинарное взыскание.

2.7. Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Филиала, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями системного администратора и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

2.8. Любой сотрудник должен согласовывать следующие действия с системным администратором:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

2.9. Ответственный за организацию обработки персональных данных не может требовать от системного администратора действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов Филиала, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение к Положению

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание