Частное образовательное учреждение
высшего образования
«Курский институт менеджмента, экономики и бизнеса»

УТВЕРЖДАЮ
Ректор ЧОУ ВО «Курский институт менеджмента, экономики и бизнеса»
приказ № 01.01-03/54 от 27.04.2024

_____В.М. Окороков
Рассмотрено и принято на заседании Ученого совета
протокол № 5 от 27.04.2024

ПОЛОЖЕНИЕ
о внутреннем аудите соответствия обработки персональных данных установленным требованиям в Частном образовательном учреждении высшего образования «Курский институт менеджмента, экономики и бизнеса»

Курск, 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о внутреннем аудите соответствия обработки персональных данных установленным требованиям (далее – Положение) определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля соответствия обработки персональных данных в Частном образовательном учреждении высшего образования «Курский институт менеджмента, экономики и бизнеса», (далее – МЭБИК) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») и принятыми в соответствии с ним правовыми актами.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами (с изменениями и дополнениями в нормативных документах).

1.3. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

2. ОБЩИЕ ТРЕБОВАНИЯ К ВНУТРЕННЕМУ АУДИТУ

2.1. Целями осуществления внутреннего аудита являются:

- оценка общего состояния выполнения в МЭБИК требований по обработке и защите персональных данных, закрепленных законодательно, а также в локальных актах МЭБИК;
- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2.2. Внутренний аудит соответствия обработки персональных данных в МЭБИК требованиям к защите персональных данных (далее – внутренний аудит) осуществляется путем проведения проверок лицом, ответственным за организацию обработки персональных данных в МЭБИК (далее – ответственный за организацию обработки персональных данных).

2.3. Ответственный за организацию обработки персональных данных назначается приказом ректора МЭБИК.

3. ПОРЯДОК ОСУЩЕСТВЕЛНИЯ ВНУТРЕННЕГО АУДИТА

3.1. Проверки соблюдения требований законодательства в сфере персональных данных разделяются на:

- плановые;
- внеплановые.

3.2. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся не реже одного раза в год.

3.3. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных.

3.4. Проведение внеплановой проверки организуется ответственным за организацию обработки персональных данных в течение трех рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных или с даты выявления нарушений установленных требований.

3.5. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка заключения по проверке.

3.6. В ходе подготовки к проведению проверки ответственный за организацию обработки персональных данных определяет:

- границы и описание области, подвергающейся проверки;
- перечень контрольных параметров;
- объекты контроля (процессы, подразделения, информационные системы персональных данных и т.п.);
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

3.7. Типовой перечень контрольных параметров приведен в приложении к настоящему Положению (Приложение 1).

3.8. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите персональных данных;
- опрос персонала, участвующего в процессах обработки персональных данных, обслуживании и эксплуатации информационных систем персональных данных.

3.9. Проверки проводятся комиссией непосредственно на месте обработки ПД путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.10. Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

3.11. Общий срок проверки не должен превышать 20 (двадцати) рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 (десять) рабочих дней.

4. ПРАВА КОМИССИИ ПРИ ПРОВЕДЕНИИ ПРОВЕРКИ

4.1. Ответственный за организацию обработки персональных данных для реализации своих полномочий имеет право:

- принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных в МЭБИК.

4.2. Проверки могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

5. ПОРЯДОК ФИКСИРОВАНИЯ РЕЗУЛЬТАТОВ ПРОВЕРКИ

5.1. Результаты проведенных проверок оформляются в виде акта внутреннего аудита, составленного по форме согласно Приложению № 2 к настоящему Положению, который подписывается ответственным за организацию обработки персональных данных или председателем комиссии и утверждается ректором МЭБИК.

5.2. По результатам проверки, при необходимости, проводится заседание. Решения, принятые на заседаниях комиссии, оформляются протоколом.

5.3. В целях контроля устранения выявленных нарушений может быть проведена повторная проверка.

Приложение № 1

ПЕРЕЧЕНЬ
контрольных параметров проверок соответствия обработки персональных данных установленным требованиям (типовой)

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в МЭБИК
2.	Подтверждение факта ознакомления с локальными актами МЭБИК в области обработки и обеспечения безопасности персональных данных
3.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных, выполнения обязанностей, предусмотренных законодательством о персональных данных
4.	Наличие законных целей и оснований обработки всех категорий персональных данных
5.	Соблюдение сроков хранения и порядка уничтожения персональных данных
6.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
7.	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

Приложение № 2

Форма акта внутреннего аудита соответствия обработки персональных данных требованиям к защите персональных данных в МЭБИК

АКТ
внутреннего аудита соответствия обработки персональных данных требованиям к защите персональных данных в Частном образовательном учреждении высшего образования «Курский институт менеджмента, экономики и бизнеса»

1. Настоящий Акт составлен в том, что «___»_____ 20__ г. ответственным за организацию обработки персональных данных проведена проверка (внутренний аудит) соответствия обработки персональных данных требованиям к защите персональных
данных в Частном образовательном учреждении высшего образования «Курский институт менеджмента, экономики и бизнеса».
2. Проверка осуществлялась в соответствии с требованиями:
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Положения об обработке и защите персональных данных работников, утв. приказом от 01.09.2022 № 140.
3. Результаты рассмотрения вопросов по предметам аудита:

Предмет аудита	Результат рассмотрения	Примечание

Выявленные нарушения:
_____
_____
_____
Меры по устранению нарушений:
_____
_____
Срок устранения нарушений:_____.