ПРАВИЛА
осуществления внутреннего контроля соответствия обработки конфиденциальной информации, в том числе персональных данных, требованиям к защите конфиденциальной информации, в том числе персональных данных, политике оператора в отношении обработки конфиденциальной информации, в том числе персональных данных

1. Настоящие правила определяют основания, форму и порядок осуществления в государственного областного бюджетного профессионального образовательного учреждения «Колледж искусственного интеллекта в машиностроительной отрасли» внутреннего контроля соответствия обработки конфиденциальной информации, в том числе персональных данных (далее – КИ), требованиям к защите КИи политике оператора в отношении обработки КИ, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ«Об информации, информационных технологиях и о защите информации» и принятыми в соответствии с ними нормативными правовыми актами.

2. Настоящие правила разработаны в соответствии с Федеральным законом Российской Федерации от 27.07.2006г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон№ 152-ФЗ), Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее – Федеральный закон № 149-ФЗ), постановлением Правительства Российской Федерации от 01.11.2012 г.№ 1119 «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства № 1119), Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - Приказ ФСТЭК России № 17).

3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

4. Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ, постановления Правительства № 1119 и Приказа ФСТЭК России № 17.

5. Внутренний контроль осуществляется путем проведения проверок не реже 1 раза в год.

6. Проверку проводит Комиссия, назначенная приказом (распоряжением) государственного областного бюджетного профессионального образовательного учреждения «Колледж искусственного интеллекта в машиностроительной отрасли» (далее – Организация или Оператор) или на договорной основе юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Состав Комиссии не менее 3-х человек, включая лицо, ответственное за организацию обработки КИ. Все члены комиссии при принятии решения обладают равными правами.

8. Комиссия при проведении проверки обязана:

- провести анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей предусмотренных Федеральным законом № 152-ФЗ(статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами оператора определяющих его политику в отношении обработки персональных данных (далее – ПДн);

- провести анализ выполнения оператором требований по определению и обеспечению уровня защищенности ПДн, утвержденных постановлением Правительства № 1119;

- провести анализ реализации оператором организационных и технических мер по обеспечению безопасности КИ, утвержденных Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- провести анализ реализации оператором организационных и технических мер по обеспечению безопасности ПДн, утвержденных приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы (далее – ИС) на соответствие Техническому паспорту ИС;

- своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите КИ, установленных законодательными и нормативными правовыми актами Российской Федерации;

- при проведении проверки соблюдать законодательство Российской Федерации, права и законные интересы оператора.

9. Комиссия при проведении проверки вправе:

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

- получать доступ к ИС в части, касающейся ее полномочий;

- принимать меры по приостановлению или прекращению обработки КИ, осуществляемой с нарушением требований к защите КИ;

- вносить руководителю организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите КИ, установленных законодательными и нормативными правовыми актами Российской Федерации.

10. При проведении проверки члены Комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;

- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

11. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется руководителю организации для принятия соответствующего решения (форма Акта приведена в приложение 1 к настоящим правилам).

12.В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты КИ, об их характере и о лицах, допустивших указанные нарушения.

13. Акт должен содержать заключение о соответствии или несоответствии обработки КИ требованиям к защите КИ и политике оператора в отношении обработки КИ, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и принятыми в соответствии с ним нормативными правовыми актами.

Лицо, ответственное за организацию
обработки конфиденциальной
информации, в том числе
персональных данных _____ С. И. Корчагин

Приложение № 1
к Правилам осуществления внутреннего контроля соответствия обработки конфиденциальной информации, в том числе персональных данных, требованиям к защите конфиденциальной информации, в том числе персональных данных, политике оператора в отношении обработки конфиденциальной информации, в том числе персональных данных

АКТ № _____
проведения внутренней проверки условий обработки конфиденциальной информации, в том числе персональных данных, в государственном областном бюджетном профессиональном образовательном учреждении «Колледж искусственного интеллекта в машиностроительной отрасли»

Дата составления: «____» _____ 20___ г.
Место проведение проверки: _____

Комиссия, назначенная приказом руководителя
от «___» _____ 20___ №_____ в составе:
Председатель
_____
Члены комиссии:
_____ -
_____ -

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки конфиденциальной информации, в том числе персональных данных, требованиям к защите конфиденциальной информации, в том числе персональных данных, политике оператора в отношении обработки конфиденциальной информации, в том числе персональных данных» провела проверку условий обработки конфиденциальной информации, в том числе персональных данных в государственном областном бюджетном профессиональном образовательном учреждении «Колледж искусственного интеллекта в машиностроительной отрасли».

В ходе проведения проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей предусмотренных Федеральным законом № 152-ФЗ (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами оператора определяющих его политику в отношении обработки персональных данных;

- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства № 1119;

- проведен анализ реализации оператором организационных и технических мер по обеспечению безопасности конфиденциальной информации, в том числе персональных данных, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- проведен анализ реализации оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: _____

ЗАКЛЮЧЕНИЕ комиссии:

Обработка конфиденциальной информации, в том числе персональных данных, соответствует (или не соответствует) требованиям к защите конфиденциальной информации, в том числе персональных данных, и политике оператора в отношении обработки конфиденциальной информации, в том числе персональных данных, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информацион-

ных технологиях и защите информации» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии _____
Члены комиссии: _____
_____

Лист ознакомлений
с правилами осуществления внутреннего контроля соответствия обработки конфиденциальной информации, в том числе персональных данных, требованиям к защите конфиденциальной информации, в том числе персональных данных

№ п/п	Фамилия, имя, отчество	Наименование подразделения, отдела	Дата ознакомления	Роспись