Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕТРОЗАВОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ПетрГУ)

ПРИКАЗ

24.12 2020 г. № 712

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня 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», в целях обеспечения безопасности персональных данных в ПетрГУ

ПРИКАЗЫВАЮ:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных (Приложение 1).
2. Утвердить состав Комиссии ПетрГУ по внутреннему контролю соответствия обработки персональных данных требованиям к защите персональных данных:
   - ответственный за организацию обработки персональных данных ПетрГУ,
   - заместитель директора РЦНИТ по развитию,
   - начальник отдела информационной безопасности.
3. Комиссии ПетрГУ по внутреннему контролю соответствия обработки персональных данных требованиям к защите персональных данных руководствоваться в своей работе Правилами осуществления внутреннего контроля соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор А. В. Воронин

Приложение №1
к приказу от «24» 12 2020 г. № 1-12

Правила осуществления внутреннего контроля соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных (далее - Правила) разработаны в целях выявления и предотвращения нарушений законодательства Российской Федерации в сфере персональных данных.

2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее - внутренний контроль) осуществляется в соответствии с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня 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" и локальными актами оператора.

3. Настоящие Правила определяют порядок осуществления внутреннего контроля в ПетрГУ и действуют постоянно.

4. В целях осуществления внутреннего контроля в ПетрГУ организовывается проведение проверок условий обработки персональных данных.

При проведении внутренней проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- соответствие полномочий обработки ПДн матрице доступа;
- соблюдение пользователями информационных систем персональных данных ПетрГУ парольной и антивирусной политики;
- обработка ПДн сотрудниками, не включенными в перечень допущенных в обработке ПДн;
- обработка ПДн после достижения цели обработки ПДн
- отсутствие подписанных обязательств о неразглашении ПДн;
- хранение файлов на рабочей станции сотрудника, содержащих ПДн;
- возможность считывания информации с экрана монитора для посторонних;
- соблюдение порядка резервирования баз данных и хранения резервных копий;
- ненадлежащее хранение бумажных носителей с персональными данными;
- соблюдение порядка доступа в помещение, в котором ведется обработка ПДн;

5. Проверки условий обработки персональных данных на соответствие требованиям к защите персональных данных (далее - проверки) осуществляются комиссией ПетрГУ по внутреннему контролю соответствия обработки персональных данных требованиям к защите персональных данных.

6. Проверки внутреннего контроля проводятся по поручению ректора ПетрГУ не реже 1 раза в два года либо в связи с поступившим в ПетрГУ обращением субъекта персональных данных о

нарушениях правил обработки персональных данных.

7. В течение трех рабочих дней с момента поступления в ПетрГУ заявления о нарушениях правил обработки персональных данных принимается решение о проведении проверки, которое оформляется распоряжением ректора ПетрГУ или распоряжением ответственного за организацию обработки персональных данных ПетрГУ.

8. Проведение проверки организуется в течение трех рабочих дней с момента оформления распоряжения ПетрГУ о проведении проверки внутреннего контроля.

9. При проведении проверки комиссией устанавливается соблюдение или нарушение правил обработки персональных данных установленным требованиям.

10. Срок проведения внеплановой проверки не должен превышать 30 календарных дней со дня регистрации обращения субъекта персональных данных.

11. При проведении проверки комиссия имеет право:

1) запрашивать у сотрудников ПетрГУ информацию, необходимую для проведения проверки;

2) привлекать к деятельности комиссии сотрудников различных отделов ПетрГУ.

3) вносить ректору ПетрГУ предложения о принятии мер (правовых, организационных, технических) по обеспечению безопасности персональных данных при их обработке;

4) вносить ректору ПетрГУ предложения о привлечении к дисциплинарной ответственности лиц, нарушивших правила обработки персональных данных.

12. Каждая проверка оформляется актом проведения проверки, соответствия обработки персональных данных требованиям к защите персональных данных. Решение комиссии оформляется протоколом проведения проверки. Форма акта и протокола приведены в приложениях к настоящим Правилам.

13. О результатах проведенной проверки и мерах, необходимых для устранения нарушений (в случае их выявления), ректору ПетрГУ докладывает ответственный за организацию обработки персональных данных ПетрГУ.

14. Членами комиссии обеспечивается конфиденциальность персональных данных, ставших известными им при проведении проверки.

15. Контроль за своевременностью и правильностью проведения назначенных проверок осуществляется ответственным за организацию обработки персональных данных ПетрГУ.

Приложение №1
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
в ПетрГУ требованиям к защите персональных данных

Акт
проведения проверки соответствия обработки
персональных данных в ПетрГУ требованиям к защите персональных данных
от "__" _____ 20__ года

Членами комиссии ПетрГУ по внутреннему контролю соответствия обработки персональных данных требованиям к защите персональных данных проведена проверка соответствия обработки персональных данных требованиям к защите персональных данных.

Тема проверки:

_____
_____

В ходе проведения проверки установлено:

Возможные нарушения требований к защите персональных данных (ПДн)	**Наличие нарушения**
соответствие полномочий обработки ПДн матрице доступа	
соблюдение пользователями информационных систем персональных данных ПетрГУ парольной и антивирусной политики	
обработка ПДн сотрудниками, не включенными в перечень допущенных в обработке ПДн	
обработка ПДн после достижения цели обработки ПДн	
отсутствие подписанных обязательств о неразглашении ПДн	
хранение файлов на рабочей станции сотрудника, содержащих ПДн	
возможность считывания информации с экрана монитора для посторонних	
не соблюдение порядка резервирования баз данных и хранения резервных копий	
ненадлежащее хранение бумажных носителей с персональными данными	
не соблюдение порядка доступа в помещение, в котором ведется обработка ПДн;	
Другое	

Рекомендации по устранению выявленных нарушений:

_____
_____
_____

Члены комиссии:
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия

Приложение №2
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
в ПетрГУ требованиям к защите персональных данных

Протокол
проведения проверки внутреннего контроля соответствия
обработки персональных данных в ПетрГУ требованиям к защите персональных данных

Настоящий Протокол составлен в том, что комиссией по внутреннему контролю соответствия обработки персональных данных в ПетрГУ требованиям к защите персональных данных проведена проверка _____.
(указывается тема проверки)

По результатам проверки составлен акт от "___" _____ 20__ г.
Проверка осуществлялась в соответствии с требованиями Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора".

В ходе проверки проверено:
_____
_____

Выявленные нарушения:
_____
_____
_____

Меры по устранению нарушений:
_____
_____

Срок устранения нарушений: до "___" _____ 20__ года.

Члены комиссии:
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия