ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

П Р И К А З

27.03. 2020 г. № 192

Об утверждении Методики
проведения внутреннего контроля
соответствия обработки и защиты ПДн

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п р и к а з ы в а ю:

1. Утвердить «Методику проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства РФ в структурных подразделениях СПбГУТ».
2. Проректору по ВРиСО Алексеенко И.А. в течение пяти рабочих дней со дня подписания приказа, утвержденную Методику разместить для свободного доступа на официальном сайте университета.
3. Контроль за исполнением приказа возложить на проректора по безопасности Пидласко Т.Н.

Приложение: 1. Методика... на 4 л.
2. Акт... на 2 л.

Ректор С.В. Бачевский

ОБЩИЙ ОТДЕЛ

Кононов Павел Александрович
8 (931) 228-26-15

Приложение № 1

УТВЕРЖДЕНА
приказом СПбГУТ
от 27.03. 2020 № 192

МЕТОДИКА
проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства РФ в структурных подразделениях СПбГУТ

1. Общие положения

1.1 Настоящая Методика определяет порядок проведения внутреннего контроля (внутренних проверок) соответствия обработки и защиты персональных данных требованиям законодательства Российской Федерации в структурных подразделениях СПбГУТ.

1.2 Методика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и техническим мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и принятыми в соответствии с ними нормативными правовыми актами.

1.3 Целью внутренних проверок является определение соответствия организации обработки и защиты персональных данных субъектов действующему законодательству РФ, а также локальным нормативным актам СПбГУТ.

1.4 Внутренний контроль соответствия обработки и защиты персональных данных в структурных подразделениях СПбГУТ требованиям законодательства РФ осуществляется комиссией, назначенной приказом СПбГУТ. По результатам проведения внутреннего контроля оформляется акт проверки с указанием мер, необходимых для устранения выявленных

нарушений. Акты о результатах проверки структурных подразделений СПбГУТ хранятся у начальника отдела ТЗИ в течение 5 лет.

1.5 В состав комиссии могут включаться работники тех структурных подразделений, в отношении которых осуществляется внутренний контроль.

1.6. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных субъектов, не раскрывают данные третьим лицам и не распространяют персональные данные без согласия субъекта.

2. Порядок проведения внутреннего контроля

2.1 Внутренние проверки проводятся в соответствии с Планом внутренних проверок соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных в структурных подразделениях СПбГУТ, утверждаемым приказом СПбГУТ. План составляется ежегодно ответственным за организацию обработки персональных данных в СПбГУТ и утверждается ректором.

2.2 Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест работников, участвующих в процессе обработки персональных данных.

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

2.4 Проведение внеплановой проверки структурных подразделений СПбГУТ на предмет соответствия обработки и защиты персональных данных требованиям законодательства РФ организуется проректором по безопасности, а в его отсутствие — начальником отдела технической защиты информации в течение 3-х рабочих дней с даты поступления письменного обращения субъекта персональных данных о нарушении правил обработки персональных данных.

2.5 При проведении внутреннего контроля используется следующий перечень контрольных параметров проверок в области обработки и защиты персональных данных:

2.5.1 соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы обработки и защиты персональных данных в структурном подразделении СПбГУТ;

2.5.2 подтверждение факта ознакомления работников структурного подразделения СПбГУТ с внутренними локальными нормативными

документами, регулирующими вопросы обработки и защиты персональных данных в СПбГУТ, а также с законодательной базой Российской Федерации.

2.5.3 решение о необходимости актуализации внутренней нормативной базы в структурном подразделении СПбГУТ;

2.5.4 порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;

2.5.5 соблюдение правил и сроков хранения материальных носителей персональных данных;

2.5.6 выборочные проверки работников на предмет знания организационно-распорядительных документов в области обработки и защиты персональных данных;

2.5.7 наличие законных целей и оснований для обработки определенных категорий персональных данных;

2.5.8 соответствие установленных должностных лиц, допущенных к обработке персональных данных, в структурных подразделениях с приказом «Об утверждении перечня лиц, допущенных к обработке персональных данных, в СПбГУТ», внесение корректировок в приказ по необходимости;

2.5.9 наличие и состояние учета съемных носителей персональных данных;

2.5.10 наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

2.5.11 соответствие полномочий пользователя информационных систем персональных данных (ИСПДн) матрице доступа к ИСПДн;

2.5.12 соблюдение пользователями ИСПДн требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн;

2.5.13 соблюдение порядка доступа в помещения, где ведется обработка персональных данных;

2.5.14 знание пользователей ИСПДн положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;

2.5.15 наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных;

2.5.16 порядок и условия применения средств защиты информации;

2.5.17 реализация рекомендаций предшествующих проверок.

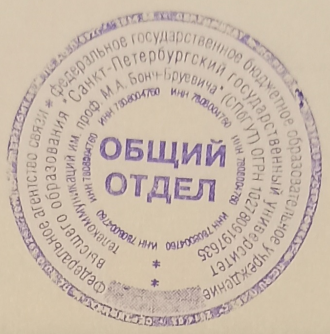
2.6 Комиссия при проведении внутреннего контроля имеет право:

2.6.1 запрашивать у руководителей структурных подразделений СПбГУТ информацию и (или) документы, необходимые для осуществления внутреннего контроля;

2.6.2 вносить предложения о совершенствовании правового, организационного и технического обеспечения безопасности персональных данных при их обработке в структурных подразделениях СПбГУТ;

2.6.3 принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных в структурных подразделениях СПбГУТ;

2.6.4 вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.



Приложение № 2

УТВЕРЖДЕН
приказом СПбГУТ
от 27.03. 2020 № 192

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

УТВЕРЖДАЮ
Руководитель организации

_____

«____» _____ 20___ г.

АКТ

_____№_____
_____

о проверке выполнения требований
законодательства РФ
о персональных данных в ….

Основание: приказ СПбГУТ от __.__.20__ № ___ «…….»
Составлен комиссией в составе:
Председатель комиссии: должность, И.О. Фамилия
Члены комиссии:
должность, И.О. Фамилия;
должность, И.О. Фамилия;
должность, И.О. Фамилия.

С __ по __ _____ 20___ года комиссией была проведена проверка
_____
_____
_____
_____
_____

В ходе проверки установлено следующее.

1. _____

2. _____

3. _____

Выводы:

1. _____

2. _____

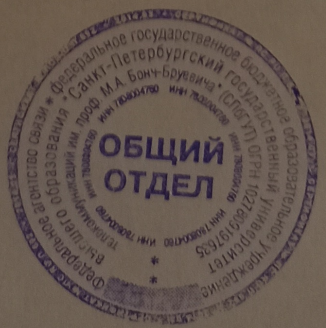
3. _____

Рекомендации:

1. _____

Акт составлен в одном экземпляре.

Председатель комиссии И.О. Фамилия

Члены комиссии: И.О. Фамилия

И.О. Фамилия