

Приложение № 1
к приказу ректора
Самарского университета
от 03 10 2017 № 770-0

Положение
о комиссии по контролю соответствия обработки и защиты
персональных данных установленным требованиям
законодательства в федеральном государственном автономном
образовательном учреждении высшего образования
«Самарский национальный исследовательский университет имени
академика С.П. Королева»

г. Самара, 2017 г.

1. Общие положения

1.1. Положение о комиссии по контролю соответствия обработки и защиты персональных данных (далее – Комиссия) установленным требованиям законодательства (далее – Положение) в федеральном государственном автономном образовательном учреждении высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (далее – университет) определяет предназначение, задачи, функции, полномочия и порядок функционирования Комиссии.

1.2. Целью создания Комиссии является контроль и координация действий руководителей структурных подразделений и должностных лиц университета, отвечающих за обработку и защиту персональных данных (далее – ПД), по обеспечению требований законодательства в области обработки и защиты персональных данных работников, обучающихся и иных категорий субъектов персональных данных.

1.3. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом 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», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Постановлением Правительства РФ от 01.11.2012 г. № 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, осуществляемых без использования средств автоматизации» и иными нормативными правовыми актами Российской Федерации, а также локальными нормативно-правовыми актами университета.

1.4. Комиссия в своей работе руководствуется Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, организационно-распорядительными документами университета и настоящим Положением.

1.5. Комиссия взаимодействует с органами, осуществляющими контроль в сфере обработки и защиты персональных данных, с администрацией и руководителями структурных подразделений университета.

1.6. Комиссия не рассматривает вопросы защиты информации, отнесенные законодательством Российской Федерации к государственной тайне.

2. Основные задачи комиссии

2.1. Контроль и координация действий должностных лиц университета по вопросам обработки и защиты персональных данных.

2.2. Разработка рекомендаций и требований к должностным лицам университета, направленных на решение следующих вопросов:

- надежное и эффективное функционирование системы обработки и защиты персональных данных;
- своевременное выявление и закрытие возможных каналов неправомерного распространения персональных данных;
- совершенствование системы организационной и технической защиты ПД, направленной на обеспечение соответствия обработки и защиты персональных данных установленным требованиям законодательства.

2.3. Проведение внутренних проверок соблюдения требований законодательства в области обработки и защиты персональных данных структурными подразделениями университета, подготовка соответствующих предложений по решению проблем в области обработки и защиты персональных данных.

3. Основные функции комиссии

3.1. Общий контроль соблюдения руководителями структурных подразделений и иными должностными лицами университета требований по обеспечению безопасности персональных данных и соблюдения требований законодательства в области обработки и защиты персональных данных, в том числе:

- контроль за подготовкой и своевременным направлением в уполномоченный орган по защите прав субъектов персональных данных информационных писем об обработке персональных данных в случае изменения сведений, содержащихся в уведомлении об обработке персональных данных;
- контроль за порядком предоставления информации (персональных данных) органам власти, физическим и юридическим лицам;
- контроль за соблюдением порядка взаимодействия с федеральными органами исполнительной власти по вопросам обработки и защиты персональных данных;
- контроль за обеспечением безопасности помещений структурных подразделений, в которых производится обработка персональных данных, а также

находятся на хранении материальные носители персональных данных и разработка мер, необходимых для обеспечения таких условий;

- контроль выполнения требований законодательства Российской Федерации, в части касающейся согласия субъектов персональных данных на обработку их персональных данных;

- контроль за соответствием используемых структурными подразделениями типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации в области персональных данных;

- контроль соответствия внутренних нормативных документов, в части касающейся обработки и защиты персональных данных требованиям законодательства Российской Федерации;

- контроль порядка и своевременности ознакомления работников университета с нормативно-правовыми актами Российской Федерации, внутренними документами университета, регламентирующими обработку и защиту персональных данных;

- контроль соответствия договорной базы университета требованиям законодательства Российской Федерации в области персональных данных;

- контроль выполнения работ по классификации (определению уровня защищенности) информационных систем персональных данных;

- контроль за проведением работ по формированию моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных университета;

- контроль за организацией работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса (уровня защищенности) информационных систем;

- контроль учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем обработки и защиты с учетом класса (уровня защищенности) информационной системы;

- контроль за соответствием условий эксплуатации информационных систем персональных данных требованиям организационно-технической и эксплуатационной документации;

- контроль соблюдения работниками организации установленных требований по обеспечению безопасности персональных данных, проведение

разбирательств и составление заключений по фактам несоблюдения данных требований;

- контроль работ по своевременному уточнению, блокированию обработки персональных данных субъектов (при необходимости) и уничтожению персональных данных (по достижении целей обработки или в случае утраты необходимости в их достижении) при их автоматизированной обработке;

- контроль обеспечения безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации;

- контроль порядка и своевременности ознакомления работников университета, осуществляющих обработку персональных данных без использования средств автоматизации, а также лиц, осуществляющих такую обработку по договору с университетом, о факте обработки ими персональных данных без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

- контроль организации раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- контроль порядка и своевременности уничтожения материальных носителей персональных данных в случае достижения целей обработки или в случае утраты необходимости в их достижении с составлением актов об уничтожении.

3.2. Планирование и проведение внутренних проверок состояния обработки и защиты персональных данных.

3.3. Анализ эффективности и достаточности принятых мер и применяемых средств обработки и защиты персональных данных.

3.4. Разработка предложений по совершенствованию системы обработки и защиты персональных данных.

3.5. Организация обучения (повышения осведомленности) и проверка знаний должностных лиц университета, допущенных к обработке ПД.

3.6. Анализ законодательства Российской Федерации в области персональных данных.

3.7. Организация работ и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

3.8. В случае выявления неправомерных действий с персональными данными направление руководителю структурного подразделения университета, допустившего нарушение, уведомления о необходимости устранения нарушения,

проведение разбирательств и составление заключений по фактам несоблюдения установленных требований.

4. Права и ответственность комиссии

4.1. Комиссия имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на неё задач;
- проводить исследование (обследование) технических и программных средств, используемых для обработки и защиты ПД в структурных подразделениях университета;
- проводить проверки соблюдения режима обработки и защиты ПД в структурных подразделениях университета;
- вносить предложения ректору университета по совершенствованию существующей системы обработки и защиты ПД;
- привлекать к работе по созданию и совершенствованию системы обработки и защиты ПД других работников университета;
- проводить служебные расследования по фактам утечки ПД или грубых нарушений режима обработки и защиты ПД;
- требовать от должностных лиц университета письменных объяснений при проведении служебных расследований;
- вносить предложения ректору университета об отстранении от выполнения служебных обязанностей должностных лиц, систематически нарушающих требования по обработке и защите ПД;
- давать должностным лицам университета обязательные для выполнения указания по обработке и защите ПД, определяемые существующим в Российской Федерации законодательством и требованиями локальных нормативно-правовых актов университета;
- привлекать в установленном порядке специалистов (работников, обучающихся и др.), имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы;
- заслушивать на заседаниях Комиссии руководителей структурных подразделений и должностных лиц, ответственных за обработку персональных данных о выполнении ими обязанностей по соблюдению режима обработки и защиты персональных данных и соблюдению гарантий прав работников, совершеннолетних обучающихся, законных представителей несовершеннолетних обучающихся и иных физических лиц на защиту персональных данных;

– участвовать в подготовке локальных нормативных актов, касающихся обработки и защиты ПД;

– вносить работодателю предложения о поощрении работников качественно соблюдающих правила по обработке и защите персональных данных;

– содействовать разрешению споров, связанных с нарушением законодательства в области обработки и защиты персональных данных.

4.2. Председатель Комиссии и члены Комиссии несут ответственность за организацию обработки и защиты персональных данных в университете в соответствии с законодательством Российской Федерации.

5. Порядок работы комиссии

5.1. Основной формой работы Комиссии является проверка.

5.2. Председатель Комиссии вносит проект плана-графика проведения внутреннего контроля соответствия обработки и защиты персональных данных в структурных подразделениях университета требованиям законодательства на рассмотрение ректору и после его утверждения организует проведение проверок в соответствии с планом-графиком.

5.3. Секретарь Комиссии отвечает за подготовку проверок, совместно с должностными лицами, проводящими проверку, оформляет акты проверки соответствия обработки персональных данных установленным требованиям законодательства, контролирует выполнение рекомендаций Комиссии по результатам проверок, готовит отчеты о работе Комиссии. Подготавливает проект плана-графика внутренних проверок структурных подразделений университета, который утверждается ректором университета и поэтапные планы внутренних проверок, которые утверждаются указанием председателя Комиссии в соответствии с приказом ректора.

5.4. Заседания Комиссии проводятся по мере необходимости, но не реже одного раза в год.

5.5. Материалы к обсуждению на заседаниях Комиссии готовятся секретарем Комиссии.

5.6. По результатам заседаний Комиссии оформляются протоколы заседаний Комиссии, которые подписываются председателем Комиссии и секретарем Комиссии.

5.7. По результатам осуществления внутреннего контроля соответствия обработки персональных данных в структурных подразделениях университета установленным требованиям законодательства составляется акт проверки соответствия обработки персональных данных в структурных подразделениях университета, который подписывается должностными лицами, проводившими

проверку, и утверждается председателем Комиссии, а в его отсутствие - заместителем председателя Комиссии.

6. Заключение

6.1. Состав Комиссии утверждается приказом ректора университета.

6.2. Предложения об изменениях и дополнениях в настоящее Положение могут вноситься: членами Комиссии, ответственным за организацию обработки персональных данных в университете, администратором безопасности персональных данных университета, администратором безопасности информационных систем персональных данных университета, ответственными за обработку персональных данных в структурных подразделениях университета и лицами, уполномоченными на получение, обработку, хранение, передачу и другое использование ПД. Работники университета могут вносить предложения об изменениях и дополнениях в настоящее Положение через ответственных за обработку персональных данных в структурных подразделениях.

Предложения об изменениях и дополнениях в настоящее Положение оформляются служебной запиской на имя ответственного за организацию обработки персональных данных в университете (председателя Комиссии).

6.3. Внесение изменений и дополнений в настоящее Положение осуществляется путём подготовки ответственным за организацию обработки персональных данных в университете (председателем Комиссии) проекта Положения в новой редакции. Проект согласовывается в установленном порядке и утверждается приказом ректора университета.