Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

ПРИКАЗ

Самара

№ 621 **- ОВ** **«**21**»** октября **2022 года**

по общим вопросам

Об утверждении локальных нормативных актов по обработке персональных данных федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет»

В целях выполнения требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

ПРИКАЗЫВАЮ:

1. Утвердить Политику обработки персональных данных в информационных системах персональных данных федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет».
2. Утвердить Положение об обеспечении безопасности персональных данных в информационных системах персональных данных федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет».
3. Утвердить Положение о хранении персональных данных в ФГАОУ ВО «СГЭУ».
4. Утвердить Положение о порядке уничтожения обрабатываемых персональных данных в информационных системах персональных данных федерального государственного автономного образовательного учреждения

высшего образования «Самарский государственный экономический университет».

5. Считать утратившим силу «Политику обработки и защиты персональных данных в ФГБОУ ВО «СГЭУ», утв. приказом от 20.01.2020г. №11-ОВ, «Правила обработки персональных данных в ФГБОУ ВО «СГЭУ», «Положение о хранении персональных данных в ФГБОУ ВО «СГЭУ», утв. Приказом от 31.08.2020г. №571-ОВ.

6. Контроль за исполнением настоящего приказа возлагаю на проректора по безопасности и управлению хозяйственным комплексом А.А. Максимова.

Врио ректора Е.А. Кандрашина

Разработал: Начальник ОИБ С.П. Ткаченко

(846) 933-88-09 (вн.502)

Федеральное государственное
автономное образовательное
учреждение высшего образования
«Самарский государственный
экономический университет»

УТВЕРЖДЕНО
приказом врио ректора
ФГАОУ ВО «СГЭУ»
№ 69-05 от 21.10. 2022 г.

ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Листов 15

Самара
2022 год

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с Перечнем присвоенных идентификаторов.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

ИСПДн	–	Информационная система персональных данных
ПДн	–	Персональные данные
РФ	–	Российская Федерация
Субъект	–	Субъект персональных данных
Университет	–	Федеральное государственное автономное образовательное Университет высшего образования «Самарский государственный экономический университет»
ФСБ России	–	Федеральная служба безопасности России
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России

1 Общие положения

Положение об обеспечении безопасности персональных данных (далее – Положение) в Федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет» (далее – Университет), расположенном по следующему адресу:

- 443090, г. Самара, ул. Советской Армии, д. 141,

определяет порядок организации работ, требования, правила и рекомендации по обеспечению безопасности персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных Федерального государственного автономного образовательного Университета высшего образования «Самарский государственный экономический университет» (далее – ИСПДн ФГАОУ ВО «СГЭУ»).

Требования настоящего Положения обязательны для их выполнения всеми сотрудниками Университета, участвующими в обработке ПДн, которые должны быть ознакомлены с Положением под роспись.

Положение разработано в соответствии со следующими нормативно-правовыми актами Российской Федерации (далее – РФ):

- Трудовой кодекс РФ;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10 июля 2014 года № 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»;

и иных нормативно-правовых документов РФ в области обработки и обеспечения безопасности ПДн.

Согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» при обработке ПДн Университет обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий.

В случае обработки ПДн с использованием средств автоматизации в Университете необходимо выполнять требования Постановления Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Общий порядок обеспечения безопасности персональных данных

Объектами защиты в Университете являются ПДн, обрабатываемые в Университете, в том числе средства и системы информатизации, в которых производится обработка ПДн (средства вычислительной техники, программные средства, обеспечивающие обработку ПДн (операционные системы, системы управления базами данных, общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для защиты ПДн, физические носители ПДн, включая бумажные.

В целях обеспечения безопасности обрабатываемых ПДн в Университете необходимо обеспечить выполнение следующих мероприятий:

- утверждение документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе персональных данных (далее – ИСПДн) Университета, необходим для выполнения ими служебных (трудовых) обязанностей;

- назначение должностного лица (сотрудника), ответственного за организацию обработки ПДн в ИСПДн Университета;
- назначение должностного лица (сотрудника), ответственного за обеспечение безопасности ПДн в ИСПДн Университета;
- назначение правил разграничения доступа к защищаемым ПДн в ИСПДн Университета;
- обеспечение сохранности носителей ПДн;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации;
- организация режима обеспечения безопасности помещений, в которых размещена ИСПДн Университета, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Функции по защите ПДн в Университете возлагаются на ответственного за обеспечение безопасности ПДн, назначенного приказом Ректора Университета.

Основными задачами данного ответственного сотрудника являются:

- ознакомление сотрудников, непосредственно осуществляющих обработку ПДн, с требованиями законодательства РФ и локальными актами Университета по обеспечению безопасности ПДн и (или) обучение сотрудников;
- применение правовых, организационных и технических мер по обеспечению безопасности ПДн в Университете;
- организация разграничения доступа к ИСПДн Университета;
- сопровождение средств защиты информации (в том числе криптографических) от несанкционированного доступа и основных технических средств, и систем;
- контроль эффективности применяемых мер защиты информации в ИСПДн Университета;
- участие в осуществлении внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону от 27 июля 2006 года № 152 «О персональных данных» и принятым в соответствии с ним нормативно-правовым актам, требованиям к защите ПДн, политике в отношении обработки ПДн и иным локальным актам Университета.

3. Определение перечня персональных данных

С целью определения перечня обрабатываемых ПДн в соответствии с Федеральным законом от 27 июля 2006 года № 152 «О персональных данных»

необходимо с установленной периодичность проводить сбор информации от специалистов структурных подразделений Университета с учетом их опыта и профессиональных знаний.

Полученную от сотрудников Университета информацию о составе обрабатываемых ПДн следует подвергать экспертной оценке ответственного за организацию обработки ПДн в ИСПДн Университета с целью установления категории обрабатываемых ПДн, по результатам которой сведения о ПДн оформляются в виде Перечня персональных данных, обрабатываемых в ИСПДн Университета.

Данный Перечень вступает в силу после его утверждения Ректором Университета и в полном объеме доводится до руководителей структурных подразделений, а также сотрудников, допущенных к обработке ПДн.

Периодичность обязательного пересмотра Перечня персональных данных, обрабатываемых в ИСПДн Университета устанавливается 1 раз в 3 года.

4. Требования к носителям персональных данных

В соответствии с Постановлением Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» необходимо обеспечивать сохранность носителей ПДн. Все места хранения материальных носителей сведений, содержащих ПДн, подлежат утверждению Ректором Университета.

Уничтожение носителя ПДн допустимо любым возможным способом, исключающим возможность дальнейшей обработки ПДн, содержащихся на этом носителе. Уничтожение ПДн на электронных носителях допустимо с помощью гарантированного удаления файлов, содержащих ПДн, без физического уничтожения носителя.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку ПДн с сохранением возможности обработки иных данных, зафиксированных на носителе.

Уничтожение носителей ПДн проводится комиссией в составе не менее 2 (двух) человек, в которой должен присутствовать ответственный за организацию обработки ПДн и ответственный за обеспечение безопасности ПДн. По результатам уничтожения оформляется Акт об уничтожении и выполняется фиксация в Журнале учета уничтожения информации на съемных носителях персональных данных.

5. Требования к размещению технических средств

Технические средства ИСПДн Университета следует размещать в помещениях, расположенных в пределах контролируемой зоны. Приказом Ректора Университета необходимо утвердить Перечень помещений, в которых осуществляется обработка ПДн.

При размещении автоматизированных рабочих мест пользователей ИСПДн Университета на нижних этажах зданий рекомендуется располагать их во внутренних помещениях, максимально удаленных от границ контролируемой зоны.

Серверное и коммуникационное оборудование ИСПДн Университета должно располагаться в отдельном помещении с запираемой дверью и замком повышенной надежности – серверной комнате. Перечень лиц, имеющих право доступа в серверную комнату, подлежат утверждению Ректором Университета. Ключи от дверей серверного помещения должны находится только у сотрудников, имеющих право доступа в него. Допускается устанавливать коммуникационное оборудование в отдельных запираемых и опечатываемых металлических шкафах, размещаемых в охраняемых помещениях.

Размещение устройств отображения и печати информации, используемых в составе ИСПДн Университета (печатающие устройства, видеотерминалы и др.), следует осуществлять с учетом максимального затруднения визуального просмотра информации посторонними лицами. Рекомендуется применять шторы, жалюзи на окнах или непрозрачные экраны.

Условия, затрудняющие несанкционированный доступ к техническим средствам ИСПДн Университета и материальным носителям ПДн при их обработке (в том числе хранении), приведены в Порядке доступа сотрудников Университета в помещения, в которых ведется обработка персональных данных.

6. Порядок доступа к информационным ресурсам

При организации правил доступа к ресурсам сетей общего пользования (Интернет) главной целью является обеспечение непрерывной и безопасной работы пользователей ИСПДн Университета.

Запрещается доступ к сети общего пользования в случае неисправности или нештатного функционирования подсистемы межсетевого экранирования, а также средств защиты информации рабочих станций пользователей (включая средства антивирусной защиты).

Доступ к ресурсам Интернет может быть блокирован ответственным за обеспечение безопасности ПДн в ИСПДн Университета без предварительного уведомления при возникновении нештатных ситуаций.

Основными средствами защиты при подключении ИСПДн Университета к сетям общего пользования являются программные, программно-аппаратные межсетевые экраны, сертифицированные по требованиям безопасности информации.

При локальном доступе к рабочим станциям, а именно при использовании локальной учетной записи для соответствующей рабочей станции, пользователям и администраторам ИСПДн Университета необходимо использовать на рабочих местах только выделенные им технические средства. При уходе с рабочего места пользователям и администраторам ИСПДн Университета следует блокировать доступ к своему автоматизированному рабочему месту.

Пользователям и администраторам ИСПДн Университета запрещается выполнять следующие действия:

- выключать антивирусное программное обеспечение и персональные межсетевые экраны на своих рабочих местах без разрешения ответственного за обеспечение безопасности ПДн в Университете;
- сообщать посторонним лицам идентификаторы и пароли доступа к персональным компьютерам;
- осуществлять доступ к персональным компьютерам других пользователей, работа с которыми не требуется в соответствии со служебными обязанностями пользователя и не санкционирована администраторами ИСПДн Университета, в том числе по своим идентификационным данным;
- осуществлять попытки несанкционированного доступа к любым объектам корпоративной сети.

7. Порядок функционирования системы защиты информации

В соответствии с Приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации, в зависимости от угроз безопасности информации, используемых

информационных технологий и структурно-функциональных характеристик ИСПДн должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Постоянный контроль работоспособности ПДн и технических средств ИСПДн ФГАОУ ВО «СГЭУ» осуществляет ответственный за обеспечение безопасности ПДн.

Периодически не реже одного раза в год ответственный за обеспечение безопасности ПДн осуществляет контроль соответствия настроек программных и технических средств и СЗИ нормативным, руководящим и эксплуатационным документам.

С целью своевременного выявления и предотвращения утечки информации, содержащей ПДн, в ИСПДн ФГАОУ ВО «СГЭУ» должен проводиться периодический контроль состояния защиты согласно утверждаемому ежегодно Плану внутренних проверок состояния защиты ПДн в ИСПДн ФГАОУ ВО «СГЭУ».

Контроль состояния защиты ПДн должен проводиться не реже одного раза в год, а также дополнительно при существенном изменении состава технических средств и систем или условий обработки информации, содержащей ПДн.

Все работы по контролю должны проводиться при строгом соблюдении мер безопасности, исключающих разглашение сведений о проводимых работах, местах размещения технических средств и систем, используемых СЗИ и возможных каналах утечки информации, содержащей ПДн.

При обнаружении нарушений при обработке ПДн в ИСПДн ФГАОУ ВО «СГЭУ» следует рассмотреть вопрос о прекращении обработки ПДн ИСПДн ФГАОУ ВО «СГЭУ» или ограничении допуска пользователей, допустивших нарушения, к обработке ПДн.

8. Ответственность за разглашение информации, содержащей персональные данные

Под разглашением информации, содержащей ПДн, понимается действие или бездействие должностных лиц, в результате которых информация, содержащая ПДн, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Утрата документов, содержащих ПДн, – это выход (в том числе и временный) документов из владения ответственного за их сохранность сотрудника, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать известны посторонним лицам.

Разглашение информации, содержащей ПДн, или утрата документов, содержащих таковую, относится к числу грубых нарушений трудового договора (контракта).

За разглашение информации, содержащей ПДн, утрату документов, содержащих такие сведения, а также за иные нарушения режима защиты ПДн, виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством РФ.