ТГСХА ТВЕРСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ АКАДЕМИЯ	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА МИНСЕЛЬХОЗ РОССИИ ФГБОУ ВО ТВЕРСКАЯ ГСХА ***Положение*** ***о персональных данных*** ***в ФГБОУ ВО Тверская ГСХА***

УТВЕРЖДАЮ:

Ректор ФГБОУ ВО Тверская ГСХА

_____ О. Р. Балаян

«__» _____ 2017 г

Приложение 1 к приказу
№ 48-0 от 26.07.2017
об утверждении Положения
о персональных данных

ПОЛОЖЕНИЕ

О ПЕРСОНАЛЬНЫХ ДАННЫХ
В ФГБОУ ВО ТВЕРСКАЯ ГСХА

Тверь 2017г.

1. Назначение и область действия Положения

Настоящее положение о персональных данных (далее - Положение) содержит общие положения, требования законодательства к организации обработки персональных данных без использования средств автоматизации, к оператору информационных систем персональных данных, описание порядка проведения классификации информационных систем и персональных данных, основные мероприятия по защите персональных данных в ФГБОУ ВО Тверская ГСХА (далее - ТГСХА), описание состава документов правового обеспечения обработки персональных данных в ТГСХА, состав персональных данных в разрезе информационных систем, характеристику типовых информационных систем персональных данных и основных угроз безопасности персональных данных, описана организационная сторона защиты персональных данных и ответственность должностных лиц по их защите.

Все работники ТГСХА должны быть ознакомлены с настоящим Положением под роспись, и сведения о факте ознакомления должны быть внесены в лист ознакомления (Приложение №1).

2. Общие положения

Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по контролю за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Роскомнадзор проводит плановые (целевые, комплексные) проверки, а также проверки по жалобам и обращениям физических и юридических лиц. Проверки систем защиты персональных данных могут также осуществляться ФСТЭК России или ФСБ России при проведении контроля систем защиты конфиденциальных данных или использования криптосредств.

Нарушение законодательства о персональных данных, в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ (ред. от 22.02.2017г.) «О персональных данных» влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, налагаемую в судебном порядке.

К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накоп-

ление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

В настоящее время законодательно-нормативная база по персональным данным включает:

- Федеральный закон от 19.12.2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 1.11.2012 г.№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства Российской Федерации от 6.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Постановление Правительства Российской Федерации от 03.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
- Приказ Россвязькомнадзора от 16.07.2010 г. № 482 «Об утверждении образца формы уведомления об обработке персональных данных».

Обеспечение безопасности персональных данных должно осуществляться в соответствии с методическими документами ФСТЭК России:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 14 февраля 2008 года.
- Приказа ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Использование криптосредств для обеспечения безопасности персональных данных должно осуществляться в соответствии с:

- Приказ ФСБ от 10 июля 2014 года 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";

- Приказ ФСБ России от 9 февраля 2005 года N 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";

- "Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденная приказом ФАПСИ от 13 июня 2001 года N 152;

- "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности", утвержденные руководством 8 Центра ФСБ России (N 149/7/2/6-432 от 31.03.2015).

На основании указанных выше документов всеми организациями и физическими лицами на территории Российской Федерации должен обеспечиваться требуемый уровень безопасности персональных данных. Лица, виновные в нарушении требований несут предусмотренную законодательством Российской Федерации ответственность.

3. Обработка персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства Российской Федерации от 15.09.2008 г №687.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливается оператором (Более подробно см. документ «Положение об обработке ПДн без использования средств автоматизации»).

4. Основные обязанности операторов информационных систем, обрабатывающих персональные данные

Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

В отношении действующих информационных систем, обрабатывающих персональные данные, операторы обязаны провести их классификацию с оформлением соответствующего акта, реализовать в установленный законом срок комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами в виде системы защиты персональных данных.

5. Порядок проведения (или уточнения) классификации информационных систем персональных данных

Постановление Правительства Российской Федерации от 01.11.2012 г № 1119 возлагает обязанность установления уровня защищенности информационных систем персональных данных и задачу обеспечения их безопасности - на оператора персональных данных, а разработку методов и способов защиты персональных данных в информационных системах - на ФСТЭК России и ФСБ России.

Операторы обязаны при обработке персональных данных принимать требуемые организационные и технические меры, в том числе при необходимости использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

6. Правовое обеспечение обработки персональных данных

Обработка персональных данных в ТГСХА производится в соответствии со следующими нормативными и организационно-распорядительными документами:

- Трудовым Кодексом Российской Федерации;
- ФЗ от 23.12.2012г. №273 «Об образовании»;
- Законом Тверской области от 07.05.2008г. № 56-ЗО «Об образовании в Тверской области»;
- ФЗ №152 «О персональных данных» от 27.07.2006;
- Постановление Правительства РФ №687 от 15.09.2008;
- Постановление Правительства РФ №1119 от 01.11.2012;
- Указ Президента РФ №609 от 30.05.2005;

7. Состав персональных данных, обрабатываемых в информационных системах

В состав информационной системы ТГСХА входит ряд ИСПДн, в которых в зависимости от выполняемых ИСПДн функций обрабатываются персональные данные из следующего списка:

- ФИО;
- Дата рождения;
- Гражданство;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Сведения о месте жительства;
- Контактный телефон;
- Социальный статус;
- Сведения страхового свидетельства государственного пенсионного страхования;
- Свидетельства о постановке на учет в налоговом органе физического лица по месту жительства;
- Сведения об образовании;
- Сведения о воинском учете;
- Сведения о ближайших родственниках
- Данные о трудовом договоре;
- Сведения о трудовом стаже;
- Сведения о расчетах и начислениях;
- ИНН;
- Суммы взносов и доход;
- Сведения о расовой и национальной принадлежности;
- Сведения о политических взглядах;
- Сведения о религиозных и философских убеждениях;
- Сведения о состоянии здоровья и личной жизни.

8. Учет и хранение документов, содержащих персональные данные

Учет и хранение в ТГСХА документов, содержащих персональные данные, следует осуществлять в соответствии с документом «Положение об обработке персональных данных без использования средств автоматизации».

9. Характеристики информационных системы персональных данных и актуальные угрозы безопасности персональным данным

Информационная система ТГСХА представляет собой совокупность взаимодействующих подсистем обработки персональных данных.

Актуальные угрозы безопасности персональных данных для ИСПДн ТГСХА определены и описаны в Моделях угроз безопасности ПДн для каждой ИСПДн.

10. Организация работ по защите персональных данных в информационной системе ТГСХА

В соответствии с законодательством Российской Федерации, защита персональных данных ТГСХА включает следующие организационные мероприятия:

- Определить (или уточнить) состав и категории обрабатываемых персональных данных;
- Определить порядок обработки персональных данных;
- Подготовить должностные инструкции сотрудников, обрабатывающих персональные данные;
- Назначить ответственных за работу с персональными данными;
- Обеспечить охрану персональных данных;
- Осуществить (или уточнить) уровень защищенности действующих информационных систем, обрабатывающих персональные данные;
- Провести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- Провести необходимые организационные и технические мероприятия для обеспечения защиты: персональных данных, обрабатываемых без использования средств автоматизации; информационных систем, обрабатывающих персональные данные;
- Провести учет лиц, допущенных к работе с персональными данными в информационной системе;
- Провести учет персональных данных, обрабатываемых в ТГСХА;
- Ввести журнал учета обращений субъектов персональных данных (Приложение №2);
- Ввести журнал учета ПДн (Приложение №3);
- Доработать План внутренних проверок состояния защиты персональных данных (См. Приложение №4);
- Ввести журнал учета ключей от помещений (Приложение №5);
- Определить перечень ПДн, обрабатываемых в ИСПДн (Приложение №6);
- Провести обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними в соответствии с документацией;

- Организовать контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- Организовать процедуру разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

11. Обязанности и ответственность должностных лиц

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке возлагается на руководителей структурных подразделений ТГСХА, администраторов локальной вычислительной сети (ЛВС), администраторов баз данных и администраторов информационной безопасности.

Кроме того, ответственность за выполнение требований настоящего Положения несут зарегистрированные пользователи.

Руководители структурных подразделений ТГСХА:

- несут ответственность за нарушения порядка допуска работника к сведениям конфиденциального характера;

- проводят регулярно, не реже одного раза в квартал, инструктаж работников ТГСХА по вопросу обеспечения защиты сведений конфиденциального характера;

- организуют выполнение требований настоящего Положения и иных нормативных документов по обеспечению режима защиты информации сотрудниками на рабочих местах;

- определяют информационные ресурсы подразделения, подлежащие защите, уязвимые места, проводят анализ риска их использования и реализации рентабельных средств защиты;

- информируют отдел информационных технологий об изменениях в статусе любого сотрудника, использующего ресурсы информационных систем.

Администратор информационной безопасности осуществляет организацию и контроль мероприятий, связанных с функционированием средств защиты персональных данных в соответствии с «Инструкцией администратора информационной безопасности», организует обучение сотрудников основам информационной безопасности.

Администратор ЛВС осуществляет организацию и контроль мероприятий, связанных с защитой информации при работе в ЛВС и использовании ресурсов ЛВС, в соответствии с «Инструкцией администратора ЛВС».

Пользователи ИСПДн отвечают за соблюдение политики информационной безопасности, принятой в ТГСХА, и докладывают руководителю структурного подразделения о любом подозрении при нарушении информационной защиты.

Пользователи ИСПДн обязаны:

- до получения доступа к конфиденциальным документам и сведениям изучить требования настоящего Положения, других нормативных документов

по защите персональных данных, действующих в ТГСХА, в части их касающейся;

- хранить в тайне персональные данные, ставшие им известными по работе или иным путем, пресекать действия других лиц, которые могут привести к разглашению персональных данных, сообщать о фактах несанкционированного доступа и действий со стороны других исполнителей, случаях утечки и разрушения обрабатываемой информации;

- знакомиться с конфиденциальными документами и сведениями, к которым получили доступ в силу своих служебных обязанностей, правильно определять конфиденциальность документов, строго соблюдать правила их пользования, порядок учета и хранения;

- при составлении конфиденциальных документов, содержащих персональные данные, ограничиваться минимальными, действительно необходимыми конфиденциальными сведениями; определять количество экземпляров конфиденциальных документов, в строгом соответствии со служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;

- при работе с конфиденциальными документами, содержащими персональные данные, на рабочем месте держать только те конфиденциальные документы, с которыми осуществляется работа; все остальные хранить в сейфе (в металлическом шкафу);

- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке и другие требования установленные ТГСХА;

- при увольнении, уходе в отпуск, отъезде в длительную командировку сдавать или отчитываться перед подразделением которое отвечает за учет и хранение конфиденциальных сведений, содержащих персональные данные, за все числящиеся за ними конфиденциальные документы;

- знакомить представителей других организаций с конфиденциальными документами, содержащими персональные данные, только по согласованию и с письменного разрешения ректора ТГСХА, при наличии документов у представителей других организаций, удостоверяющих их личность;

Пользователям ИСПДн запрещается:

- сообщать свои пароли кому бы то ни было, и разрешать входить в сеть под своим именем; подбирать или отгадывать чужие пароли;

- изменять конфигурационную настройку операционной системы; добавлять, изменять или удалять программное обеспечение, отдельные компоненты операционной системы;

- модифицировать чужие файлы, если по каким-то причинам у них есть доступ на запись;

- использовать персональные данные в открытых документах, на автоматизированных рабочих местах, не предназначенных для обработки (хранения) персональных данных;

- сообщать устно или письменно посторонним лицам персональные данные;

- выполнять работы, связанные с обработкой персональных данных, на дому;
- снимать копии с документов, содержащих персональные данные, или производить выписки из них без письменного разрешения руководителя подразделения;
- передавать и принимать без росписи документы, содержащие персональные данные;
- уничтожать самостоятельно (без согласования с руководителем подразделения) персональные данные;
- несанкционированно тиражировать, передавать и модифицировать программные средства защиты информации.

Детальные обязанности работников ТГСХА в части защите информации должны быть указаны в должностных инструкциях и положениях о соответствующих подразделениях. Допуск работников к работе с ПДн проводится в соответствии с Инструкцией по учету лиц, допущенных к обработке ПДн.

Отказ соблюдать настоящее Положение может подвергнуть защищаемую информацию ТГСХА недопустимому риску потери конфиденциальности, целостности или доступности при ее хранении, обработке или передаче.

При выявлении фактов нарушения прав доступа к сведениям конфиденциального характера руководителям структурных подразделений ТГСХА необходимо немедленно информировать об этом ректора или его заместителя. По всем выявленным фактам проводятся служебные разбирательства с выяснением причин и обстоятельств произошедшего и с принятием дисциплинарных мер в отношении виновных нарушителей. При этом учитывается, что работники ТГСХА, разгласившие сведения конфиденциального характера, а также работники, по вине которых произошла утеря документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами ТГСХА и условиями трудового договора.

Приложение № 1
к Положению о персональных данных

Лист ознакомления

С Положением о персональных данных в ФГБОУ ВО Тверская ГСХА, утвержденным приказом №___ от « »_____20__ г. ознакомлены:

№ п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение №2
к Положению о персональных данных

Журнал учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных

№ п/п	ФИО субъекта ПДн	Дата обращения	Цель обращения

Приложение №3
к Положению о персональных данных

Журнал учета персональных данных

№ п/п	Дата, № согласия	Субъект ПДн (Ф.И.О.)	Перечень ПДн, на обработку которых дается согласие субъекта	Цель обработки ПДн	Срок, в течение которого действует согласие	Подпись лица, получившего согласие

Приложение №4
к Положению о персональных данных

План внутренних проверок состояния защиты персональных данных

Мероприятие	Периодичность	Исполнитель
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Контроль над соблюдением режима защиты	Ежедневно	
Контроль над выполнением антивирусной защиты	Еженедельно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
Проведение обследований на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	

Приложение №5
к Положению о персональных данных

Журнал учета ключей

№ ключа	Помещение	Ф.И.О. получателя	Дата выдачи	Подпись получателя	Примечание

Приложение №6
к Положению о персональных данных

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в информационных системах персональных данных
ФГБОУ ВО Тверская ГСХА

№ п/п	Наименование сведений	Субъекты ПДн	Наименование ИСПДн, где возможна обработка ПДн	Типы документов, где возможно появление ПДн
КАТЕГОРИЯ 3 (К3) **персональные данные, позволяющие идентифицировать субъекта ПД**				
	ФИО, паспортные данные, ИНН, сведения об образовании	Абитуриент	Объединенная ИСПДн на базе ИС «КиберДИПЛОМ» и ИС «Приемная комиссия»	Личное дело абитуриента, свидетельство ЕГЭ, экзаменационные ведомости, сводные ведомости на зачисление, отчеты
	ФИО, паспортные данные, ИНН, суммы взносов и доход	Сотрудник	ИСПДн СБиС++ версия 2	Документы финансового характера
	ФИО, паспортные данные, ИНН, сведения об образовании	Сотрудник	Локальный документооборот	

КАТЕГОРИЯ 2 (К2) **персональные данные, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию**				
	ФИО, паспортные данные, финансовая информация, сведения о месте жительства, контактный телефон, социальный статус, сведения страхового свидетельства государственного пенсионного страхования, свидетельства о постановке на учет в налоговом органе физического лица по месту жительства, сведения о воинском учете, сведения о ближайших родственниках, данные о трудовом договоре, сведения о трудовом стаже, сведения о расчетах и начислениях.	Сотрудник	ИСПДн бухгалтерского и кадрового учета на базе ИС 1С:Зарплата и кадры бюджетного учреждения 8 и ИС 1С:Бухгалтерия государственного учреждения 8	Личные дела и трудовые книжки сотрудников, кадровые документы (Табеля, приказы, больничные листы, документы финансового характера (расчетные листки, расчетно-платежные ведомости)