ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени И.С.Тургенева

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени И.С. ТУРГЕНЕВА»
(ОГУ им. И.С.Тургенева)

04.07.2016. **П Р И К А З** № 311

Об утверждении инструкций
по защите информации

В целях выполнения требований «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 20.08.2002 года № 282, Постановления Правительства Российской Федерации от 01.11.2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказов ФСТЭК России от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также других нормативных документов Российской Федерации и Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева) в области безопасности информации,

п р и к а з ы в а ю:

1. Утвердить инструкцию по парольной защите в автоматизированных информационных системах ОГУ имени И.С. Тургенева (далее – АИС), в том числе в информационных системах персональных данных (далее – ИСПДн) - Приложение1.
2. Утвердить инструкцию по антивирусной защите в АИС, ИСПДн ОГУ имени И.С. Тургенева – Приложение 2.
3. Утвердить инструкцию пользователя АИС, ИСПДн ОГУ имени И.С. Тургенева, в которых осуществляется обработка информации ограниченного доступа, в том числе персональных данных и конфиденциальной информации - Приложение 3.

4. Утвердить правила обработки персональных данных в ОГУ имени И.С. Тургенева – Приложение 4

5. Контроль за исполнением настоящего приказа возложить на директора департамента информатизации и перспективного развития А.В. Коськина.

6. Приказ довести до сотрудников ОГУ имени И.С. Тургенева в части касающейся.

И.о. ректора О.В. Пилипенко

СОГЛАСОВАНО:

И.о. первого проректора А.А. Федотов

Директор департамента внутреннего административного контроля С.И. Ягупов

Начальник ПУ Т.И. Ератова

Проект приказа вносит Директор Департамента информатизации и перспективного развития А.В. Коськин

Приложение 1
утверждена Приказом ОГУ имени И.С. Тургенева
от 04.07.2016 года № 311

ИНСТРУКЦИЯ
по парольной защите в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированных информационных системах (далее – АИС) Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева), в том числе в информационных системах персональных данных – ИСПДн, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех АИС и ИСПДн ОГУ имени И.С. Тургенева и контроль за действиями исполнителей и обслуживающего персонала АИС и ИСПДн ОГУ имени И.С. Тургенева при работе с паролями возлагается на Администратора безопасности информации.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 8 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение Администратору безопасности информации.

Опечатанные конверты с паролями исполнителей должны храниться в сейфе.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий должна производиться Администратором безопасности информации немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий Администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Приложение 2
утверждена Приказом ОГУ имени И.С. Тургенева
от 04.07.2016 года № 311

ИНСТРУКЦИЯ
по антивирусной защите в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора безопасности информации Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева).

К применению в автоматизированных информационных системах ОГУ имени И.С. Тургенева (далее – АИС), в том числе в информационных системах персональных данных – ИСПДн, допускаются сертифицированные ФСБ и/или ФСТЭК России антивирусные средства.

На АРМ АИС используются только лицензионные антивирусные средства.

Настройка параметров средств антивирусного контроля осуществляется администратором безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая на съемных носителях (магнитных дисках, CD-ROM, флэш памяти и т.п.).

Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля.

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

При работе с внешними носителями информации пользователи обязаны перед их применением осуществить проверку их на предмет отсутствия компьютерных вирусов.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователи АИС должны провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении внеочередной антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

провести лечение или уничтожение зараженных файлов;

в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, проинформировать Администратора безопасности информации для организации дальнейших действий по его изоляции.

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящей Инструкции возлагается на Руководителя структурной службы ОГУ имени И.С. Тургенева, в котором функционирует АИС.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на Администратора безопасности информации и всех сотрудников подразделения, являющихся пользователями АИС.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделения, эксплуатирующего АИС, осуществляетс Администратора безопасности информации.

В АИС запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

Приложение 3
утверждена Приказом ОГУ имени И.С. Тургенева
от 04.07.2016 года № 311

ИНСТРУКЦИЯ
по работе пользователей в автоматизированной информационной системе Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева»

Допуск пользователей для работы в автоматизированных информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – АИС), в том числе в информационных системах персональных данных – ИСПДн, осуществляется в соответствии с приказом Федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева) и разрешительной системой доступа, установленной в ОГУ имени И.С. Тургенева.

Пользователь АИС имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение пользователю АИС полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в АИС осуществляется при первичной регистрации пользователя Администратором безопасности информации.

Пользователь АИС отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в АИС.

Вход пользователя АИС в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется Инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в полгода) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем АИС самостоятельно.

При работе со съемными носителями информации пользователь АИС каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

Пользователь АИС обязан:

- знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;
- обеспечить правильность вводимых данных;
- своевременно сообщать Администратору безопасности информации об изменениях статуса пользователя;
- незамедлительно сообщить руководителю своего структурного подразделения и Администратору безопасности информации факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю АИС запрещается:

- использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, за исключением выделенных каталогов;
- осуществлять попытки несанкционированного доступа к ресурсам операционной системы;
- в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;
- пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;
- покидать помещение с незаблокированной учетной записью;
- отключать установленные средства защиты информации;
- использовать машинные носители без их предварительной проверки антивирусными средствами;
- устанавливать программное обеспечение;
- менять параметры конфигурации ранее установленных программных средств;
- использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу;
- запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам;
- хранение пароля на любых носителях, позволяющих другим лицам получить информацию о пароле;
- использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет пользователь АИС.

Возможность получения технического доступа к конфиденциальной информации не дает права пользователям АИС обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей АИС к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Пользователь АИС несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

При нарушениях пользователем АИС правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Приложение 4
утверждены Приказом ОГУ имени И.С. Тургенева
от 04.07.2016 года № 311

ПРАВИЛА
обработки персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева»

1. Общие положения

1.1. Правила обработки персональных данных устанавливают единый порядок обработки персональных данных в Федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – Правила).

1.2. Правила разработаны на основании и в соответствии с требованиями следующих законодательных и нормативных правовых актов Российской Федерации:

- Трудовой кодекс Российской Федерации (ст. 65, ст.85-90);
- Гражданский кодекс Российской Федерации, Часть 1 (ст. ст. 150, 152, 152.1) от 30.11.1994 №51-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами;
- Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Правила устанавливают и определяют:

1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;

2) цели обработки персональных данных;

3) содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) сроки обработки и хранения обрабатываемых персональных данных;

6) порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.4. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.5. Федеральное государственное бюджетное образовательное учреждение высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее – ОГУ имени И.С. Тургенева) является оператором персональных данных, осуществляющим обработку персональных данных сотрудников, студентов, абитуриентов ОГУ имени И.С. Тургенева и граждан, обращающихся в ОГУ имени И.С. Тургенева (далее – Оператор).

1.6. Доступ к Правилам неограничен, так как Правила являются документом, определяющим политику Оператора в отношении обработки персональных данных.

1.7. Правила являются обязательными для исполнения всеми сотрудниками ОГУ имени И.С. Тургенева, имеющими доступ к персональным данным.

1.8. Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

2. Процедуры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных

2.1. Оператор при обработке персональных данных должен руководствоваться принципами и условиями, определенными нормами главы 2 Федерального закона № 152-ФЗ.

2.2. Права субъектов персональных данных определены в главе 3 Федерального закона № 152-ФЗ.

2.3. При определении обязанностей Оператора при сборе персональных данных и при обращении к нему субъектов персональных данных Оператор должен руководствоваться главой 4 Федерального закона № 152-ФЗ.

2.4. Оператор должен принимать меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, в частности:

- назначить ответственного за организацию обработки персональных данных в ОГУ имени И.С. Тургенева;
- издать документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ «О персональных данных»;
- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора;
- оценивать вред, который может быть причинён субъектам персональных данных в случае нарушения законодательства Российской Федерации и настоящих Правил;
- ознакомить сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных и настоящими Правилами;
- запрещать обработку персональных данных лицами, не допущенными к их обработке.

2.5. Обработка персональных данных должна осуществляется после получения согласия субъекта персональных данных (за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона № 152-ФЗ «О персональных данных»), при условии выполнения требований к защите персональных данных.

2.6. Безопасность персональных данных, при их обработке в информационной системе, обеспечивает Оператор.

2.7. При обработке персональных данных необходимо соблюдать следующие требования:

- к работе с персональными данными допускаются только лица, назначенные соответствующим приказом (распоряжением) ректора ОГУ имени И.С. Тургенева.
- в целях обеспечения сохранности документов, содержащих персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками ОГУ имени И.С. Тургенева, осуществляющими

данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных регламентах (инструкциях);

- на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации.

2.8. Особенности обработки персональных данных с использованием средств автоматизации

2.8.1. Обработка персональных данных с использованием средств автоматизации осуществляется в информационных системах персональных данных, состав которых должен быть определен в Перечне информационных систем персональных данных.

2.8.2. Машинные носители персональных данных должны подлежать обязательной регистрации и учету, в соответствии с Приказом ОГУ имени И.С. Тургенева, регламентирующим порядок учета и хранения носителей персональных данных.

2.8.3. Обработка персональных данных должна осуществляться при условии выполнения требований к защите персональных данных, утвержденных постановлением Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.8.4. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Состав и содержание таких мер утвержден приказом ФСТЭК России 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».

2.9. Особенности обработки персональных данных без использования средств автоматизации

2.9.1. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, изложены в постановлении Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.9.2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации:

- персональные данные при их обработке должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях;

- при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы;

- для обработки различных категорий персональных данных для каждой категории персональных данных должен использоваться отдельный материальный носитель;

- лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется 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 ОГУ имени И.С. Тургенева;

- требования к типовым формам документов, характер информации в которых предполагает или допускает включение в них персональных данных, изложены в п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства от

15 сентября 2008 года № 687;

- уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

2.9.3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации:

- обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ;

- необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3. Цели обработки персональных данных

3.1. Цель обработки персональных данных определяется целями создания и видами деятельности ОГУ имени И.С. Тургенева, а именно:

- обеспечение соблюдения законов и иных нормативных правовых актов в связи с выполнений функций по предназначению ОГУ имени И.С. Тургенева;

- соблюдение порядка и правил приема на работу и исполнение условий трудового договора, установленных трудовым законодательством Российской Федерации;

- заполнение и использование базы данных автоматизированной информационной системы бухгалтерского учета, персонифицированного учета, налогового учета, в целях повышения эффективности, быстрого поиска, формирования отчётов.

3.2 . Субъектами, персональные данные которых обрабатываются для указанных целей, являются обучающиеся ОГУ имени И.С. Тургенева и работники ОГУ имени И.С. Тургенева, принимаемые в ОГУ имени И.С. Тургенева по трудовому договору, а так же поступающие в ОГУ имени И.С. Тургенева и другие лица, обратившиеся в ОГУ имени И.С. Тургенева за трудоустройством и предоставлением услуг.

4. Содержание обрабатываемых персональных данных для каждой цели обработки персональных данных

4.1. Содержание обрабатываемых персональных данных должно определяться целью обработки персональных данных и утверждаться локальным актом Оператора (Перечень персональных данных, обрабатываемых в ОГУ имени И.С. Тургенева в связи с реализацией трудовых отношений, а также в связи с оказанием услуг и т.п.).

4.2. Содержание обрабатываемых персональных данных определяется для каждой цели обработки персональных данных.

5. Категории субъектов, персональные данные которых обрабатываются:

1) сотрудники Оператора, состоящие с ним в трудовых отношениях.

2) лица, обратившиеся в ОГУ имени И.С. Тургенева по вопросам, касающимся установленной сферы ее деятельности.

6 . Сроки обработки и хранения обрабатываемых персональных данных

6.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.3. Основания для прекращения обработки персональных данных и сроки их уничтожения определены в частях 3, 4, 5 статьи 21 Федерального закона № 152-ФЗ.

6.4. Основанием (условием) прекращения обработки персональных данных также является ликвидация в ОГУ имени И.С. Тургенева.

6.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3, 4, 5 статьи 21 Федерального закона № 152-ФЗ, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований

7.1. При уничтожении материальных носителей, содержащих персональные данные, должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

7.2. При необходимости уничтожения части персональных данных уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.3. Уничтожение части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.4. Для уничтожения персональных данных Оператор создает комиссию. В состав комиссии включается ответственный за защиту информации. Уничтожение персональных данных производится в присутствии всех членов комиссии.

7.5. После уничтожения материальных носителей членами комиссии подписывается Акт об уничтожении персональных данных и в Журнале учета материальных носителей персональных данных, а также в номенклатурах и описях дел проставляется отметка «Уничтожено, Акт №__ «___» _____ 201__ г.».

8. Ответственность за нарушение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

8.1. Лица, виновные в нарушении требований Федерального закона № 152-ФЗ, несут предусмотренную законодательством Российской Федерации ответственность.

9. Заключительные положения

9.1. Сотрудники, определенные приказом ОГУ имени И.С. Тургенева как пользователи, участвующие в обработке персональных данных, должны ознакомиться с настоящими Правилами обработки персональных данных.

9.2. Обязанность доводить до сведения сотрудников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных лежит на лице, ответственном за защиту информации (п. 2, часть 4, статья 22.1 Федерального закона № 152-ФЗ).