МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.И. ЛЕНИНА»
(ИГЭУ)

П Р И К А З

От 23 ноября 2017 года **г. Иваново** **№ 201**

О введение в действие
«Положения об обработке и защите
персональных данных в ИГЭУ»

Во исполнение требований главы 14 Трудового кодекса Российской Федерации и Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных» и в целях приведения локальных нормативных актов ИГЭУ в соответствие с действующим законодательством Российской Федерации,

ПРИКАЗЫВАЮ:

1. Ввести в действие с 01 декабря 2017 года прилагаемое «Положение об обработке и защите персональных данных в ИГЭУ» (далее Положение).
2. Руководителям структурных подразделений принять Положение к руководству и исполнению, а также ознакомить с ним под роспись всех работников и обучающихся до 31.12.2017.
3. Управлению кадров знакомить под роспись лиц, принимаемых на работу (до подписания трудового договора) с настоящим Положением.
4. Признать утратившим силу «Положение об обработке и защите персональных данных работников и студентов в ИГЭУ»», утвержденное 11 января 2012г.
5. Контроль за исполнением настоящего Приказа оставляю за собой.

Ректор **С.В.Тарарыкин**

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ)

УТВЕРЖДАЮ
Ректор ИГЭУ
_____ Тарарыкин С.В.
«23» ноября 2017 г.

Положение
об обработке и защите персональных данных в ИГЭУ

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных в ИГЭУ (далее — Положение) разработано в соответствии со следующими нормативными документами:
- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Уставом ИГЭУ;
- иными локальными нормативными актами ИГЭУ.

1.2. Положение устанавливает порядок получения, учета, обработки, накопления, хранения, уничтожения документов, содержащих сведения, отнесенные к персональным данным в федеральном государственном бюджетном образовательном учреждении высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (далее — ИГЭУ, университет).

1.3 Цель настоящего Положения — определение порядка обработки персональных данных, обеспечение защиты персональных данных от несанкционированного доступа и разглашения, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих порядок обработки и защиты персональных данных.

1.4. Настоящее Положение и изменения к нему утверждаются ректором университета и вводятся в действие приказом.

2. Основные понятия.

2.1. Для целей настоящего Положения используются следующие основные понятия:

2.1.1. *Персональные данные* — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.1.2. *Субъект персональных данных (далее Субъект ПДн)* – работник, обучающийся и иное лицо, к которому относятся соответствующие персональные данные. *Работник* –

физическое лицо, вступившее в трудовые отношения с университетом. *Обучающийся* – студент, аспирант, слушатель, учащийся подготовительных курсов, зачисленный приказом ректора в университет для обучения. *Иные лица* – физические лица (заказчик, потребитель, исполнитель, арендатор, подрядчик и др.), состоящие в договорных и иных гражданско-правовых отношениях с университетом; родственники работников и обучающихся; уволенные работники; лица поступающие в ИГЭУ (абитуриенты); лица окончившие обучение; соискатели ученой степени кандидатов наук, докторов наук; участники конференций, семинаров, фестивалей, конкурсов, олимпиад проводимых в ИГЭУ; посетители, являющиеся читателями библиотеки.

2.1.3. *Оператором*, организующим и осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, является федеральное государственное бюджетное образовательное учреждение высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ).

2.1.4. *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, анализ, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.1.5. *Автоматизированная обработка персональных данных* - обработка персональных данных с помощью средств вычислительной техники.

2.1.6. *Сбор персональных данных* – накопление информации на материальных носителях и (или) в автоматизированных информационных системах.

2.1.7. *Распространение персональных данных* - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.1.8. *Предоставление персональных данных* — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.1.9. *Блокирование персональных данных* — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.1.10. *Уничтожение персональных данных* — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.1.11. *Обезличивание персональных данных* — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.1.12. *Информационная система персональных данных* — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.1.13. *Трансграничная передача персональных данных* - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.2. Цель обработки персональных данных - оформление трудовых отношений; ведение кадровой и бухгалтерской документации; учет работников и обучающихся; осуществление образовательной деятельности по образовательным программам; оформление договорных отношений; обеспечения личной безопасности работников и обучающихся; оказание услуг по доступу к библиотекам; предоставление услуг проживания в общежитиях, регистрация граждан по месту пребывания; осуществления контроля за достоверностью сведений об участии в едином государственном экзамене граждан, поступающих в ИГЭУ; оказание медицинских услуг; оказание услуг связи; осуществление хозяйственной

деятельности; организации и осуществления работы диссертационных советов, ведение дел соискателей ученой степени; допуск к работе со сведениями, составляющими государственную тайну.

2.3. Правовое основание обработки персональных данных в ИГЭУ:
ст.ст. 23, 24 Конституции Российской Федерации; ст.ст. 5 - 22.1 Федерального закона от 27.07.06 № 152-ФЗ "О персональных данных"; ст.ст. 85 - 90 Трудового кодекса Российской Федерации; Налоговый кодекс Российской Федерации; Бюджетный кодекс Российской Федерации; Федеральный закон от 06.12.11 №402-ФЗ «О бухгалтерском учете»; Федеральный закон от 17.12.01 №173-ФЗ «О трудовых пенсиях в Российской Федерации»; Федеральный закон от 15.12.01 №167-ФЗ «Об обязательном пенсионном страховании в российской Федерации»; Федеральный закон от 01.04.96 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»; Федеральный закон от 24.07.09 №212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»; Федеральный закон от 29.12.12 №273-ФЗ «Об образовании в Российской Федерации»; ст. 53 Федерального закона от 07.07.2003 № 126-ФЗ "О связи"; Постановление Правительства РФ «О Федеральной информационной системе государственной научной аттестации» №1035 от 18 ноября 2013г.; Постановление Правительства Российской Федерации от 31.08.2013 № 755 "О ФИС и РИС обеспечения проведения ГИА обучающихся и приема граждан в ОО"; Постановление Правительства Российской Федерации от 26.08.13 №729 «О федеральной информационной системе "Федеральный реестр сведений о документах об образовании и (или) квалификации, документах об обучении"»; Федеральный закон от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации"; Федеральный закон от 22.10.2004 №125-ФЗ "Об архивном деле в Российской Федерации"; Федеральный закон от 29.12.1994 №78-ФЗ "О библиотечном деле"; Федеральный закон от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан Российской Федерации"; Гражданский кодекс Российской Федерации; Федеральный закон от 23.08.1996 №127-ФЗ "О науке и государственной научно-технической политике"; Федеральный закон от 21.12.1996 №159-ФЗ "О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей"; Федеральный закон от 21.07.1993 №5485-I "О государственной тайне"; Федеральный закон от 18.07.2006 №109-ФЗ "О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации"; Федеральный закон от 28.03.1998 №53-ФЗ "О воинской обязанности и военной службе"; Устав ИГЭУ.

3. Общие требования при обработке персональных данных.

3.1. Приказом ректора в Университете назначаются лица, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных Субъектов ПДн.

3.2. Уполномоченные лица при обработке персональных данных обязаны соблюдать следующие общие требования:

3.2.1. При определении объема и содержания обрабатываемых персональных данных необходимо руководствоваться Конституцией Российской Федерации, трудовым кодексом РФ, Федеральным законом от 27.07.06 № 152-ФЗ "О персональных данных" и иными действующими нормативно-правовыми актами РФ.

3.2.2. Обработка персональных данных осуществляется с письменного согласия Субъекта ПДн на обработку его персональных данных (Приложение №1, Приложение №2). Согласие на обработку персональных данных может быть отозвано Субъектом ПДн путем подачи письменного заявления.

3.2.3. Обработка персональных данных без согласия Субъекта ПДн может осуществляться в следующих случаях:

- в целях исполнения трудового договора, договора на обучение и (или) гражданско-правового договора, стороной которого является субъект персональных данных;

- в статистических и научных целях при условии обязательного обезличивания данных;

- для защиты жизни, здоровья и иных жизненно важных интересов Субъекта ПДн, если получение его согласия невозможно;

- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законодательством.

3.2.4. Обработка персональных данных Субъектов ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе; обеспечения личной безопасности; контроля прохождения обучения, количества и качества выполняемой работы; осуществления оплаты труда и выплаты стипендий; обеспечения сохранности имущества университета и Субъекта ПДн.

3.3. Персональные данные предоставляются самим Субъектом ПДн. Если персональные данные возможно получить только у третьей стороны, то Субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение №3). Лицо, уполномоченное на получение и обработку персональных данных, должно сообщить Субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, университет обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.4. Университет не имеет права получать и обрабатывать персональные данные Субъекта ПДн касающиеся расовой, национальной принадлежности политических взглядов, религиозных или философских убеждений, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации ИГЭУ вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.5. ИГЭУ не имеет права получать и обрабатывать персональные данные Субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.6. При принятии решений, затрагивающих интересы Субъекта ПДн, университет не имеет права основываться на персональных данных работника и обучающегося, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.7. Работник и обучающийся должен предоставлять ИГЭУ достоверные сведения о себе и своевременно, в течение 14 календарных дней, сообщать ему об изменении своих персональных данных. Для проверки достоверности уполномоченное лицо должно сверять данные, предоставленные Субъектом ПДн, с оригиналами имеющихся у него документов.

3.8. Предоставление работником подложных документов при поступлении на работу является основанием для расторжения трудового договора.

4. Состав персональных данных. Обработка персональных данных.

4.1. Комплекс документов, содержащих персональные данные, сопровождающий процесс оформления трудовых отношений работника в ИГЭУ при его приеме, переводе и увольнении:

4.1.1. Информация, представляемая работником при поступлении на работу в ИГЭУ, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета — для военнообязанных и лиц, подлежащих призыву на военную службу;

- документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;

- сведения о профессии, специальности работника;

- справку о наличии (отсутствии) судимости;

- данные о прохождении предварительного медицинского осмотра;

- в отдельных случаях, с учетом специфики работы, действующим законодательством РФ может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов (например, сведения о социальных льготах, о семейном положении работника и членах его семьи, дающих основание для предоставления работникам гарантий и компенсаций, предусмотренных законодательством (наличие и возраст детей, состояние здоровья членов семьи, наличие у работника иждивенцев, о необходимости ухода за больным членом семьи, инвалидности и др.)).

4.1.2. В Университете в работе по учету кадров используется Унифицированная форма Т-2 «Личная карточка работника», утвержденная постановлением Госкомстата Российской Федерации от 05.01.2004 (далее УФ №Т-2) в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (фамилия, имя, отчество работника, дата рождения, место рождения, пол, табельный номер, гражданство, образование, профессия, номер страхового свидетельства государственного пенсионного страхования, ИНН, стаж работы, состояние в браке и состав семьи, паспортные данные, адрес регистрации по месту жительства, адрес фактического проживания, номер контактного телефона);

- данные о приеме на работу.

В дальнейшем в личную карточку вносятся:

-сведения о переводах на другую работу;

-сведения о прохождении аттестации;

- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных льготах;

- сведения об увольнении.

4.2. Комплекс документов, сопровождающий процесс зачисления на учебу, прохождения обучения и отчисления из университета:

4.2.1. При поступлении на учебу абитуриент представляет в приемную комиссию ИГЭУ следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;

- документ об образовании;

- медицинская справка установленного образца;

- фотографии;

- другие документы, необходимые в отдельных случаях с учетом специфики поступления в ИГЭУ и действующим законодательством Российской Федерации (например, поступления в ИГЭУ иностранных граждан, детей-сирот, военнослужащих и т.д., а так же документы о результатах олимпиад, спортивных достижениях, сведения об ограничениях по здоровью и прочее).

4.2.2. После того, как будет принято решение о зачислении на учебу, а также впоследствии в процессе учебы, к документам, содержащим персональные данные обучающегося, также будут относиться:

- приказ о зачислении на учебу, о прохождении учебы, об отчислении из ИГЭУ;

- приказы о поощрениях и взысканиях;

- медицинская справка формы 086У, медицинские справки для предоставления академического отпуска;

- удостоверение гражданина, подлежащего призыву на военную службу или военный билет;

- приказы о назначении стипендии и материальном поощрении;

- личная карточка студента;

- учебная карточка студента (форма №14);

- другие документы.

4.3. На каждого работника и обучающегося в университете формируется в установленном порядке личное дело. Личные дела работников и обучающихся ведутся сотрудниками управления кадров, личные дела аспирантов и докторантов – сотрудниками управления аспирантуры и докторантуры. В их обязанности входит:

- приобщение текущих документов к личным делам;

- обеспечение сохранности личных дел;

-обеспечение конфиденциальности сведений, содержащихся в личных делах в соответствии с федеральными законами и иными нормативно-правовыми актами РФ, а также в соответствии с настоящим Положением.

Медицинские справки формы 086У на бумажных носителях хранятся в санатории-профилактории ИГЭУ (здравпункт) в запирающихся шкафах.

Учебные карточки обучающихся (форма №14) ведутся работниками учебно-методического управления и передаются в управление кадров при отчислении обучающегося из ИГЭУ для приобщения к личному делу обучающегося.

4.4. Университет осуществляет обработку персональных данных родственников работников ИГЭУ в объеме, предусмотренном УФ №Т-2. Также персональные данные родственников работников и обучающихся обрабатываются в целях оформления социальных выплат (персональные данные, содержащиеся в свидетельстве о заключении брака, свидетельстве о расторжении брака, свидетельстве о рождении детей и др.), заключения договоров об оказании платных образовательных услуг.

4.5. Сведения о воинском учете военнообязанных запаса и призывников обрабатываются сотрудниками Второго отдела ИГЭУ.

Во Втором отделе создаются и хранятся следующие группы документов, содержащие данные о работниках и обучающихся в единичном или сводном виде:

- справочно-информационный банк данных работников и обучающихся для ведения воинского учета (картотеки, журналы);

- переписка с военными комиссариатами;

- копии отчетов, направляемых в военные комиссариаты, вышестоящие органы управления и др. учреждения.

4.6. Обработка персональных данных Субъектов ПДн в ИГЭУ осуществляется с использованием средств автоматизации или без использования таких средств (на бумажных носителях).

5. Передача и хранение персональных данных

5.1. Передача персональных данных.

5.1.1. При передаче персональных данных Субъектов ПДн университет должен соблюдать следующие требования:

- не раскрывать третьим лицам и не распространять персональные данные без письменного согласия Субъекта ПДн (Приложение №4), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта ПДн, а также в других случаях, предусмотренных федеральными законами;

- не сообщать персональные данные Субъекта ПДн в коммерческих целях без его письменного согласия;

- предупредить лиц, получивших персональные данные Субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные Субъекта ПДн, обязаны соблюдать режим секретности (конфиденциальности).

Данное положение не распространяется на обмен персональными данными Субъектов ПДн в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным Субъекта ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Субъекта ПДн, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника и обучающегося, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции /возможности продолжения обучения;

- передавать персональные данные работника и обучающегося представителям работников и обучающихся в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

5.1.2. Согласие Субъекта ПДН не требуется при получении, в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

5.1.3. Персональные данные работника и обучающегося могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Субъекта ПДн, если иное не установлено законодательством РФ.

5.1.4. Передача персональных данных между структурными подразделениями осуществляется в соответствии с «Инструкцией о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные» (Приложение №5).

5.2. Хранение, уничтожение персональных данных Субъектов ПДн.

5.2.1. Персональные данные Субъектов ПДн хранятся:

- на бумажных носителях в Управлении кадров, в Управлении аспирантуры и докторантуры, в Управлении бухгалтерского учета и контроля, в Финансово-экономическом управлении, во Втором отделе, в учебно-методическом управлении, в подразделениях университета осуществляющих обучение по программам дополнительного профессионального образования и профессиональной переподготовки, в других подразделениях, с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных;

- в электронном виде - в автоматизированных информационных системах.

Перечень информационных систем персональных данных (ИСПДн), обрабатывающих персональные данные в ИГЭУ, а также места хранения баз данных утверждаются приказом ректора.

5.2.2. Персональные данные абитуриентов до зачисления в университет хранятся в Приемной комиссии ИГЭУ. После зачисления персональные данные абитуриентов передаются в управление кадров. Персональные данные не поступивших абитуриентов (личное дело, содержащее заявление и копии документов), хранятся в приемной комиссии в течение 6 месяцев с начала учебного года, затем уничтожаются, о чем составляется соответствующий документ. Оригиналы документов абитуриентов, не поступивших в ИГЭУ, хранятся в Приемной комиссии до окончания срока хранения в соответствии с законодательством РФ.

5.2.3. Хранение персональных данных Субъектов ПДн в структурных подразделениях ИГЭУ, сотрудники которых имеют право на обработку персональных данных, осуществляется в порядке, исключающем их утрату или неправомерное использование.

Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается на руководителей структурных подразделений ИГЭУ.

5.2.4. Личные дела и документы, содержащие персональные данные Субъектов ПДн, хранятся в сейфах или иных закрывающихся на замок шкафах, трудовые книжки - в металлических, несгораемых шкафах в помещениях, обеспечивающих защиту от несанкционированного доступа (помещения оснащаются охранной сигнализацией; ключи от входных дверей в нерабочее время сдаются под охрану в дежурно-диспетчерскою службу ИГЭУ в отдельных опечатанных пеналах с указанием времени приема-сдачи в журналах под роспись; ключи выдаются работникам университета по служебным удостоверениям в соответствии с утвержденным списком лиц, которым разрешен доступ в данное помещение).

5.2.5. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только работниками ИГЭУ, осуществляющими данную работу в соответствии со своими должностными обязанностями, зафиксированными в их должностных инструкциях.

5.2.6. Личные дела работников и обучающихся, первичная учетная документация по учету труда и его оплаты, документы по учету использования рабочего времени, а также иные документы, содержащие персональные данные Субъектов ПДн, по истечении сроков хранения в структурных подразделениях ИГЭУ подлежат передаче на хранение в архив ИГЭУ или уничтожению. Сроки хранения документов утверждены Номенклатурой дел ИГЭУ. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований закреплен в «Инструкции по делопроизводству» ИГЭУ.

6. Доступ к персональным данным. Защита персональных данных.

6.1. Право доступа к персональным данным Субъектов ПДн имеют:

- ректор;
- проректора (в соответствии с приказом «О распределении обязанностей между проректорами ИГЭУ»);
- главный бухгалтер;
- начальник управления кадров.

Руководители структурных подразделений имеют право доступа к персональным данным работников своего структурного подразделения, а также к персональным данным обучающихся и иных лиц в соответствии со своими должностными обязанностями.

6.2. Процедура оформления допуска сотрудников ИГЭУ к обработке персональных данных Субъектов ПДн:

- предоставление руководителями структурных подразделений ИГЭУ в Управление кадров сведений об обработке персональных данных Субъектов ПДн осуществляемой без использования средств автоматизации и с использованием средств автоматизации (Приложения № 6,7);
- на основании предоставленных от руководителей структурных подразделений сведений, утверждение приказом ректора перечня сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным;
- дополнение должностных инструкций сотрудников, допущенных к обработке персональных данных, функциональными обязанностями о необходимости соблюдения настоящего Положения.

6.3. Работники ИГЭУ, имеющие доступ к персональным данным и допущенные к их обработке должны быть ознакомлены под роспись с «Инструкцией о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные» (Приложение № 5), «Инструкцией пользователя при обработке персональных данных на объектах вычислительной техники» (Приложение № 8), а также обязаны принимать необходимые организационные и технические меры для защиты персональных данных от

неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

6.4. Уполномоченные лица имеют право обрабатывать только те персональные данные Субъектов ПДн, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

6.5. Ответы на письменные запросы других организаций и учреждений в пределах их компетенций и представленных полномочий даются в письменной форме на бланке университета и в том объеме, который позволяет не разглашать излишний объем персональных данных Субъектов ПДн. Учет информации, предоставляемой по запросам, ведется уполномоченным лицом в журнале учета передачи персональных данных. (Приложение №9).

6.6. Передача информации, содержащей сведения о персональных данных, по телефону, факсу, электронной почте без письменного согласия Субъекта ПДн запрещается.

6.7. Защита сведений, хранящихся в электронных базах данных ИГЭУ, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа пользователей, аутентификацией (пароль, логин) пользователей, использованием средств криптографической защиты информации и антивирусных программ, учетом электронных носителей.

6.8. Порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации определен в «Инструкции по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных» (Приложение №10).

6.9. В целях обеспечения защиты персональных данных Субъект ПДн имеет право:

6.9.1. Получать свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Сведения должны быть предоставлены Субъекту ПДн университетом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.9.2. Требовать от ИГЭУ уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.9.3. Получать от университета:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

6.9.4. Требовать извещения университетом всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.9.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия ИГЭУ при обработке и защите его персональных данных.

6.10. Защита персональных данных Субъекта ПДн от неправомерного их использования или утраты обеспечивается за счёт средств университета в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными

актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями ИГЭУ (Приложения № 5,8,10).

6.11. Лицом, ответственным за организацию обработки персональных данных Субъектов ПДн назначается начальник Управления кадров. Ему устанавливается следующий круг обязанностей:

- осуществлять внутренний контроль за соблюдением университетом и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников и обучающихся ИГЭУ положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

6.12. Лицом, ответственным за организацию обеспечения безопасности автоматизированной обработки персональных данных назначается начальник Управления телекоммуникаций. Ему устанавливается следующий круг обязанностей:

- осуществлять определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- осуществлять организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- проводить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- осуществлять учет машинных носителей персональных данных;
- принимать меры к обнаружению и устранению фактов несанкционированного доступа к персональным данным, а также осуществлять восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- устанавливать правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивать регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- осуществлять контроль за техническими мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

7. Ответственность за нарушение норм и правил, регулирующих обработку и защиту персональных данных

Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных работников

Я, _____ ,
(фамилия, имя, отчество)

документ, удостоверяющий личность _____
(наименование документа, серия, номер)

выдан _____
(кем, когда)

проживающий(ая)_____

даю согласие федеральному государственному бюджетному образовательному учреждению высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ) (ул.Рабфаковская, д.34, г.Иваново) на обработку своих персональных данных, то есть любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, анализ, систематизацию, накопление, обобщение, хранение, уточнение, дополнение, изменение, извлечение, использование, блокирование, удаление, уничтожение персональных данных, а также передачу персональных данных, если это необходимо для поддержания функционирования информационных систем обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности ИГЭУ в случаях, установленных нормативными документами и законодательством РФ, **при условии соблюдения всех требований по защите персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и «Положением об обработке и защите персональных данных в ИГЭУ».**

Обработка персональных данных осуществляется с целью оформления трудовых отношений, ведения кадровой и бухгалтерской документации, учета работников; осуществления образовательной деятельности по образовательным программам, обеспечения личной безопасности работников, а также наиболее полного исполнения ИГЭУ обязательств и компетенций в соответствии с законодательством Российской Федерации.

Перечень персональных данных:

1. Фамилия, имя, отчество
2. Год, месяц, дата и место рождения
3. Пол
4. Документ, удостоверяющий личность (паспорт, военный билет, вид на жительство – серия и номер документа, кем и когда выдан)
5. Гражданство
6. Адрес регистрации по месту жительства, адрес фактического проживания
7. Контактные телефоны
8. Номер страхового свидетельства государственного пенсионного страхования
9. Сведения об образовании, профессии, о квалификации или наличии специальных знаний; о присуждении ученой степени кандидата/доктора наук, номер диплома кандидата/доктора наук; сведения об ученом звании доцента/профессора, номер аттестата доцента/профессора
10. Должность, место работы, структурное подразделение, табельный номер
11. Стаж работы
12. Семейное положение
13. Сведения воинского учета
14. Результаты предварительного и ежегодного медицинского обследования, состояние здоровья (информация о заболеваниях, инвалидности)
15. Социальные льготы
16. Награды (поощрения), почетные звания
17. Адрес электронной почты
18. Доходы, сведения о банковских картах
19. Сведения о налоговых льготах
20. Справка о наличии (отсутствии) судимости
21. ИНН

Мое согласие действует в течение всего срока работы в ИГЭУ, а также после прекращения работы в течение срока, установленного законодательством РФ и локальными нормативными актами, и может быть мною отозвано путем подачи письменного заявления.

С «Положением об обработке и защите персональных данных в ИГЭУ» ознакомлен (а).

Обязуюсь своевременно, в течение 14 календарных дней, сообщать в управление кадров об изменении своих персональных данных с предоставлением оригиналов документов.

Подпись работника _____ /_____ Дата «____»_____20___г.
ФИО

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных обучающихся

Я, _____ ,
(фамилия, имя, отчество)

документ, удостоверяющий личность _____
(наименование документа, серия, номер)

выдан _____
(кем, когда)

проживающий(ая)_____

даю согласие федеральному государственному бюджетному образовательному учреждению высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ) (ул.Рабфаковская, д.34, г.Иваново) на обработку своих персональных данных, то есть любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, анализ, систематизацию, накопление, обобщение, хранение, уточнение, дополнение, изменение, извлечение, использование, блокирование, удаление, уничтожение персональных данных, а также передачу персональных данных, если это необходимо для поддержания функционирования информационных систем обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности ИГЭУ в случаях, установленных нормативными документами и законодательством РФ, **при условии соблюдения всех требований по защите персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и «Положением об обработке и защите персональных данных в ИГЭУ».**

Обработка персональных данных осуществляется с целью ведения кадровой и бухгалтерской документации; учета обучающихся; осуществления образовательной деятельности по образовательным программам, обеспечения личной безопасности обучающихся, а также наиболее полного исполнения ИГЭУ обязательств и компетенций в соответствии с законодательством Российской Федерации.

Перечень персональных данных:

1. Фамилия, имя, отчество
2. Год, месяц, дата и место рождения
3. Пол
4. Документ, удостоверяющий личность (паспорт, военный билет, вид на жительство – серия и номер документа, кем и когда выдан).
5. Гражданство
6. Адрес регистрации по месту жительства, адрес фактического проживания, сроки регистрации по месту пребывания
7. Контактные телефоны
8. Адрес электронной почты
9. Сведения об образовании
10. Свидетельство о результатах единого государственного экзамена
11. Сведения воинского учета
12. Социальные льготы
13. Фотографии
14. Курс, группа, факультет, данные о прохождении обучения, успеваемость
15. Номер зачетной книжки, номер читательского билета
16. Семейное положение
17. Стипендия, материальные поощрения, сведения о банковских картах
18. Медицинская справка по форме 086У; состояние здоровья (информация о заболеваниях, инвалидности)
19. Сведения о документе, подтверждающем право на пребывание (проживание) в РФ
20. Сведения о нуждаемости в общежитии
21. Сведения о наличии особых прав при приеме на обучение

Мое согласие действует в течение всего срока обучения в ИГЭУ, а также после прекращения учебы в течение срока, установленного законодательством РФ и локальными нормативными актами, и может быть мною отозвано путем подачи письменного заявления.

С «Положением об обработке и защите персональных данных в ИГЭУ ознакомлен(а)».

Обязуюсь своевременно, в течение 14 календарных дней, сообщать в управление кадров об изменении своих персональных данных с предоставлением оригиналов документов.

Подпись _____ / _____ / «____»_____20___г.
(ФИО)

Приложение № 3
к «Положению об обработке и защите персональных данных в ИГЭУ»

СОГЛАСИЕ
на получение персональных данных у третьих лиц

Я	зарегистрированный (ая) по адресу
паспорт	

даю согласие федеральному государственному образовательному учреждению высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ, ул. Рабфаковская, д.34, г. Иваново) на получение следующих моих персональных данных:
- фамилия, имя, отчество;
-
-
-
-
-

для _____
(указать цель обработки персональных данных)

у _____
(наименование организации)

Я также утверждаю, что ознакомлен(а) с возможными последствиями моего отказа дать письменное согласие на их получение.

_____ _____ _____
(дата) (подпись) (ФИО)

Приложение № 4
к «Положению об обработке и защите персональных данных в ИГЭУ»

СОГЛАСИЕ
на передачу персональных данных третьей стороне

Я	зарегистрированный (ая) по адресу
паспорт	

даю согласие федеральному государственному образовательному учреждению высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ, ул. Рабфаковская, д.34, г. Иваново) на предоставление

_____
(кому)

следующих моих персональных данных:
- фамилия, имя, отчество;
-
-
-
-

для _____
(указать цель предоставления персональных данных)

_____

Согласие действует в течение _____с момента его выдачи.

_____ _____ _____
(дата) (подпись) (ФИО)

Приложение № 5
к «Положению об обработке и защите персональных данных в ИГЭУ»

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ивановский государственный энергетический
университет имени В.И. Ленина» (ИГЭУ)

УТВЕРЖДАЮ
Ректор ИГЭУ
_____ Тарарыкин С.В.
«23» ноября 2017 г.

Инструкция
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1. Общие положения

1.1. Настоящей Инструкцией определяются обязательные для всех структурных подразделений университета требования по обеспечению конфиденциальности документов, содержащих персональные данные.

1.2. Для целей настоящей Инструкции используются следующие основные понятия:

- «Персональные данные» - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- «Оператором», организующим и осуществляющим обработку персональных данных, является федеральное государственное бюджетное образовательное учреждение высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ).

- «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, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- «Конфиденциальная информация» – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

1.3. Нормативными документами, определяющими основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.4. Обеспечение конфиденциальности персональных данных не требуется в случае их обезличивания или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники), в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, занимаемая должность и место работы, ученая степень, ученое звание, сведения о квалификации, профессии - для сотрудников; курс, группа, факультет, специальность, данные об обучении – для студентов и иные персональные данные, предоставленные субъектом персональных данных.

1.5. Обработка персональных данных допускается с согласия субъекта персональных данных на обработку его персональных данных.

1.6. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем подачи письменного заявления.

1.7. Порядок ведения перечней персональных данных.

1.7.1. В структурных подразделениях ИГЭУ должны формироваться и вестись перечни персональных данных с указанием регламентирующих документов, мест хранения и ответственных за обработку и хранение данных (*Приложения №6, №7 к «Положению об обработке и защите персональных данных в ИГЭУ»*). На основании предоставленных от руководителей структурных подразделений сведений, приказом ректора утверждается перечень сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным.

1.7.2. Осуществлять обработку и хранение персональных данных, не внесенных в перечень, запрещается.

1.8. Общие правила хранения и передачи персональных данных.

1.8.1. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

1.8.2. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

1.8.3. Передача персональных данных допускается только в случаях, установленных Федеральным законам Российской Федерации «О персональных данных», а также по письменному поручению (резолюции) вышестоящих должностных лиц.

1.8.4. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.9. Ответственность за защиту обрабатываемых персональных данных.

1.9.1. Лица, осуществляющие обработку и хранение персональных данных, несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством РФ.

1.9.2. Сотрудники ИГЭУ, допущенные к обработке персональных данных, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией.

1.9.3. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается на руководителей структурных подразделений ИГЭУ.

2. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации

2.1. Условия хранения персональных данных.

2.1.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, 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.

2.1.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Документы должны храниться в надежно запираемых шкафах и сейфах. Ключи от них, а также от помещений должны находиться у ответственных за данную работу лиц.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

2.1.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе

персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.1.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающее одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.2. Использование типовых форм документов и журналов учета.

2.2.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Оператора;
б) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
в) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.2.2. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится Оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится Оператор.

2.3. Порядок уничтожения или обезличивания персональных данных.

2.3.1. Уничтожение или обезличивание 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).

2.3.2. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации 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.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации.

3.1. Правила доступа, хранения и пересылки персональных данных.

3.1.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

3.1.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.1.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

3.1.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.1.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.2. Общие требования по защите персональных данных в автоматизированных системах.

3.2.1. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

3.2.2. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.2.3. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных.

3.2.4. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту.

4.2. При использовании съемных носителей персональных данных запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой

информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

4.3. Съемные носители подлежат периодической проверке на вирусы и вредоносное программное обеспечение администратором, ответственным за защиту персональных данных в структурном подразделении.

4.4. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт.

4.5. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению в установленном порядке.

Приложение № 6
к «Положению об обработке и защите персональных данных в ИГЭУ»

Сведения об обработке персональных данных работников и обучающихся ИГЭУ, осуществляемой **без использования средств автоматизации** в _____
(наименование структурного подразделения)

Перечень обрабатываемых персональных данных (указать наименование типовой формы или вида документов – картотека, журнал, книга. реестр и т.д.) **	Цель обработки персональных данных	ФИО и должность лиц, осуществляющих обработку и имеющих доступ к персональным данным	Место хранения (корпус, кабинет, сейф, специально оборудованный шкаф и др.)

«___»_____20___г. _____/_____
(Подпись) (Ф.И.О. руководителя подразделения)

Приложение № 7
к «Положению об обработке и защите персональных данных в ИГЭУ»

Сведения об обработке персональных данных работников и обучающихся ИГЭУ, осуществляемой **с использованием средств автоматизации** в _____
(наименование структурного подразделения)

Перечень обрабатываемых персональных данных	Цель обработки персональных данных	ФИО и должность лиц, осуществляющих обработку и имеющих доступ к персональным данным	Наименование информационной системы с указанием используемых программных средств. Место установки (корпус, кабинет)	Исходные данные классификации информ. системы				ФИО администратора информационной системы
				Структура инф.системы (распределенная, автономная, локальная)	Наличие подключений к сетям общего пользования (да, нет)	Режим обработки персональных данных (многопользовательский, однопользовательский)	Разграничение доступа пользователей (да, нет)	

«___»_____20_____г. _____/_____
(Подпись) (Ф.И.О. руководителя подразделения)

Приложение № 8
к «Положению об обработке и защите персональных данных в ИГЭУ»

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ивановский государственный энергетический
университет имени В.И. Ленина» (ИГЭУ)

УТВЕРЖДАЮ
Ректор ИГЭУ
_____ Тарарыкин С.В.
«23» ноября 2017 г.

Инструкция
пользователя при обработке персональных данных на объектах вычислительной техники

1. Общие положения

1.1. Настоящей Инструкцией определяются основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) ИГЭУ.

1.2. Общие требования к пользователю:

- пользователь должен быть допущен к обработке соответствующих категорий персональных данных на основании приказа ректора и иметь навыки работы на ПЭВМ;
- пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ, и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Обязанности пользователя

2.1. Пользователь обязан выполнять общие требования по обеспечению режима конфиденциальности проводимых работ:

- при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц *или* располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнение" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий,
- помнить личные пароли, не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

2.2. 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.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

2.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:
- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.4. При работе с персональными данными запрещается:
- записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;
- самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

3. Права пользователя ПЭВМ

Пользователь имеет право:
- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

4. Ответственность пользователей ПЭВМ

4.1. Пользователь несет ответственность за:
– надлежащее выполнение требований настоящей инструкции;
– соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;
– сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;
– сохранность персональных данных.

4.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных, несут предусмотренную законодательством Российской Федерации ответственность.

5. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

Приложение № 9
к «Положению об обработке и защите персональных данных в ИГЭУ»

ЖУРНАЛ УЧЕТА ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

_____ год

№	Сведения о запрашивающем лице	Состав запрашиваемых данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/ отказа в передаче персональных данных	Подпись ответственного сотрудника

Приложение №10
к «Положению об обработке и защите персональных данных в ИГЭУ»

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ)

УТВЕРЖДАЮ
Ректор ИГЭУ
_____ Тарарыкин С.В.
«23» ноября 2017 г.

Инструкция

по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

1. Общие положения.

Предметом инструкции является порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации.

2. Мониторинг аппаратного обеспечения.

Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы системных администраторов.

3. Мониторинг парольной защиты.

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей;
- периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. Мониторинг целостности.

Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мониторинг попыток несанкционированного доступа.

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

6. Мониторинг производительности.

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

7. Системный аудит.

7.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

7.2. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

7.3. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

7.4. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

8. Антивирусный контроль

Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется системным администраторами в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено системным администратором на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено системным администратором на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

9. Анализ инцидентов

Если системный администратор, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (далее НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.