ПРИНЯТО
Ученым советом ФГБОУ ВО «БГИТУ»
25 октября 2018 г.
Протокол № 3

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «БГИТУ»
_____ В.А. Егорушкин
«25» октября 2018 г.

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «Брянский государственный инженерно-технологический университет»

Версия 02

Дата введения: «29» октября 2018 г.

Брянск 2018

Должность	*Ф.И.О.*	*Подпись*	*Дата*
Проректор по Э и Ф	*Кузнецов С.Г.*		24.10.18
Начальник отдела информатизации	*Маринин И.В.*		24.10.18
Начальник отела ЛА и УКО	*Захаров Н.Е.*		24.10.18
Начальник юридического отдела	*Дячук Н.В.*		24.10.18

1. Общие положения

1.1. Настоящее положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «Брянский государственный инженерно-технологический университет» (далее – Положение) определяет порядок выполнения мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ФГБОУ ВО «БГИТУ» (далее – Оператор).

1.2. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

1.3. Положение обязательно для исполнения всеми лицами, непосредственно осуществляющими защиту персональных данных. Нарушение правил защиты персональных данных, определённых Положением, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

1.4. Настоящее Положение вступает в силу после его утверждения руководителем Оператора и введения в действия приказом руководителя Оператора. Все изменения в Положение вносятся на основании решения руководителя Оператора в установленном порядке.

2. Основные понятия

В Положении используются следующие основные понятия (выдержка из ФЗ-152):

2.1. персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2. оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с

персональными данными;

2.3. 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;

2.4. автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

2.5. распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.6. предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.7. блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.8. 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;

2.9. обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

2.10. информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

2.11. трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Информационные системы

3.1. Информационные системы, используемые в БГИТУ для хранения, обработки и передачи персональных данных: Tandem University, 1С, Сбербанк Business Online, Система передачи данных Московского индустриального банка, СБиС, АП БГИТА АС ЕГИСМ.

3.2. Локальными информационными системами являются Tandem University и 1С; данные заносятся с бумажных носителей в специальных средах лица, с определенным набором прав и полномочий. Предоставление определенного набора прав происходит посредством ввода индивидуального логина и пароля.

3.3. Информационная система «1С: Предприятие 8.3» служит для расчёта заработной платы, отчислений с заработной платы, учёт рабочего времени сотрудников и содержит следующие персональные данные сотрудников:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- место рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- телефон субъекта персональных данных;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- ИНН субъекта персональных данных;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа

об образовании, квалификация, специальность по документу об образовании);

- сведения об ученой степени звании;
- информация о гражданстве;
- медицинское заключение по установленной форме;
- табельный номер субъекта персональных данных;
- должность субъекта персональных данных;
- номер приказа и дату приема на работу (перевод, увольнение) субъекта персональных данных.

3.4. Информационная система «Tandem University» служит для автоматизации учета документов, их обработки, взаимодействия сотрудников, контроля и анализа исполнительской дисциплины и содержит персональные данные сотрудников:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- место рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- телефон субъекта персональных данных;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- ИНН субъекта персональных данных;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- сведения об ученой степени звании;

- информация о гражданстве;
- табельный номер субъекта персональных данных;
- должность субъекта персональных данных;
- приказы о предоставлении отпуска работнику, о переводе работника на другую работу, о прекращении (расторжении) трудового договора с работником (увольнении), о применении дисциплинарного взыскания, о поощрении и награждении;
- распоряжения.

3.5. Информационная система сайта Университета служит для хранения данных на официальном сайте www.bgitu.ru и содержит следующие категории персональных данных:

- ФИО;
- год рождения;
- сведения об образовании и профессии;
- ученая степень;
- ученое звание;
- занимаемая должность;
- преподаваемые дисциплины;
- наименование направления подготовки и (или) специальности;
- данные о повышении квалификации и (или) профессиональной переподготовке;
- общий стаж работы;
- стаж работы по специальности;
- сведения о местах учебы и работы;
- список публикаций;
- сведения о доходах руководящих лиц;
- фотография.

А также во время проведения приемной кампании:

- списки абитуриентов;
- сведения о результатах экзаменов.

3.6. Срок хранения персональных данных в информационных системах определен текущей номенклатурой дел.

3.7. Системы, Сбербанк Business Online, Система передачи данных

Московского индустриального банка, СБиС, АП БГИТА АС ЕГИСМ являются лишь средами передачи персональных данных, средством электронного документооборота БГИТУ с государственными службами и другими юридическими лицами.

4. Возложение ответственности за обеспечение безопасности ПДн

4.1. Для каждой из ИСПДн, в отношении которой установлена необходимость обеспечения **3 уровня защищённости**, руководителем Оператора назначается должностное лицо, ответственное за обеспечение безопасности персональных данных при их обработке в данной ИСПДн (далее – Ответственное лицо за ИСПДн). При этом одно должностное лицо может, является ответственным за обеспечение безопасности персональных данных при их обработке в нескольких ИСПДн.

4.2. Оператор определяет и осуществляет организационные и технические мероприятия, необходимые и достаточные в соответствии с требованиями действующего законодательства РФ для обеспечения безопасности персональных данных при их обработке в ИСПДн.

4.3. Оператор устанавливает требования к организационным и техническим мероприятиям, которые должна выполнять организация, осуществляющая доступ к ИСПДн Оператора.

5. Основные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн

5.1. Оператор самостоятельно или с привлечением внешней организации, обладающей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации, обязано определить необходимый уровень защищённости ПДн при их обработке в каждой из ИСПДн, оператором которой он является.

5.2. Оператор самостоятельно или с привлечением организации, обладающей лицензиями на деятельность по технической защите конфиденциальной информации и на деятельность по выполнению работ и оказанию услуг в области шифрования информации, определяет и осуществляет

организационные и технические мероприятия, которые должны выполняться Оператором для нейтрализации угроз ПДн, признанных актуальными.

5.3. Оператор обязан разработать и утвердить Требования к организационным и техническим мероприятиям, которые накладываются на организации, имеющие доступ в ИСПДн Оператора. Для разработки вышеуказанных Требований может привлекаться внешняя организация, обладающая лицензиями, необходимыми для проведения данных работ.

5.4. Оператор должен обеспечить выполнение следующих основных мероприятий:

5.4.1. Организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5.4.2. Обеспечение сохранности носителей персональных данных.

5.4.3. Актуальность утвержденного руководителем Оператора ИСПДн документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей.

5.4.4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, при этом сертификаты на средства защиты информации должны быть действительными.

5.4.5. Назначение Ответственного лица для каждой ИСПДн Оператора.

5.5. Лицо, ответственное за организацию обработки персональных данных, получив информацию о факте нарушения действующих законодательных норм по обеспечению безопасности персональных данных в ИСПДн Оператора, организует служебное расследование для выявления лиц, в результате действий или бездействия которых произошло нарушение законодательных норм по обеспечению безопасности персональных данных.

Приложение 1. Форма «Журнала поэкземплярного учета ЭЦП, эксплуатационной и технической документации к ним, ключевых документов» (для обладателя конфиденциальной информации)

№ п/п по журналу	Описание носителя и подпись	Владелец ЭЦП	Полномочия	Начало срока действия
1	2	3	4	5

Окончание срока действия	Серийный номер	PIN	Место установки использования	Дата установки
6	7	8	9	10

Ответственное должностное лицо (ФИО)	Место хранения машинного носителя	Уничтожена/действует	Сведения об уничтожении машинных носителей, стирании информации (номер акта, подпись, дата)
11	12	13	14

Приложение 2. Форма «Журнала учета СКЗИ, эксплуатационной и технической документации к ним»

ФИО пользователя	Должность, каб.	Роспись	ОС ПК	Наименование СКЗИ	S/N лицензии и другая регистрационная информация	Установлено (дата, роспись)
1	2	3	4	5	6	7