МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о.ректора УлГТУ

_____ А.П.Пинков

«10» 06 2015 г.

ПОЛОЖЕНИЕ

о работе с персональными данными в информационных системах Ульяновского государственного технического университета

1. Общие положения

Настоящее Положение регулирует отношения, связанные с обработкой персональных данных, включающие в себя производимые Ульяновским государственным техническим университетом (далее УлГТУ) действия по получению, хранению, комбинированию, передаче персональных данных или иному их использованию, с целью их защиты от несанкционированного доступа, а также неправомерного их использования и утраты.

2. Понятие и состав персональных данных

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

2.2. К персональным данным, в том числе относятся:

- анкетные и биографические данные;
- паспортные данные;
- сведения о воинском учете;
- специальность и занимаемая должность;
- сведения о заработной плате;
- сведения о социальных льготах;
- адрес места жительства, контактный телефон;
- содержание трудового договора;
- личное дело и трудовая книжка.

2.3 Работники УлГТУ, получившие по служебной необходимости доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Обработка персональных данных

3.1. 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.

3.2. УлГТУ при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.3. Допуск лиц в помещения, в которых размещена информационная система персональных данных и/или осуществляется обработка персональных данных (возможен доступ к персональным данным), осуществляется на основании служебных записок с визой проректора по режиму и безопасности. В нерабочее время помещения, в которых размещена информационная система персональных данных и/или осуществляется обработка персональных данных (возможен доступ к персональным данным), подлежат охране. При этом все окна и двери в смежные помещения должны быть надежно закрыты. Охрана помещений, в которых размещена информационная система персональных данных и/или осуществляется обработка персональных данных (возможен доступ к персональным данным), осуществляется службой проректора по режиму и безопасности.

3.4. Приказом ректора создается рабочая группа, в составе которой уполномоченные лица осуществляют:

- внутренний контроль и (или) аудит соответствия обработки персональных данных федеральному законодательству, требованиям к защите персональных данных, политике УлГТУ в отношении обработки персональных данных, настоящему Положению.
- оценку эффективности принимаемых мер по обеспечению безопасности персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровню защищенности информационной системы персональных данных УлГТУ;
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- мероприятия по обнаружению фактов несанкционированного доступа к персональным данным и информируют рабочую группу о факте несанкционированного доступа к персональным данным;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О защите персональных данных», соотношение указанного вреда и принимаемых УлГТУ мер, направленных на обеспечение выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом «О защите персональных данных».

Порядок работы рабочей группы определяется распоряжением первого проректора - проректора по научной работе.

3.5. Полномочия (роли) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (инструкции) утверждаются распоряжением первого проректора-проректора по научной работе.

4. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

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

Разработал:
Заместитель начальника управления информатизации
по информационной безопасности
_____ А.О.Серебрянников
«__»_____ 2015г.

Согласовано:
Первый проректор - проректор по научной работе
_____ Н.Г.Ярушкина
«____»_____ 2015г.

Согласовано:
Начальник управления информатизации
_____ С.К.Киселев
«__»_____ 2015г.

Согласовано:
Проректор по режиму и безопасности
_____ Л.С.Ямпольский
«____»_____ 2015г.

Согласовано:
Проректор по экономике и финансам
_____ Г.Н.Платов
«__»_____ 2015г.

Согласовано:
Начальник юридического управления
_____ Ю.В.Плюснина
«__»_____ 2015г.

Приложение № 1
к Положению о работе с персональными данными
в Ульяновском государственном техническом университете

Технические требования к информационной системе персональных данных

1. При обработке персональных данных (ПДн) в локальных информационных системах персональных данных УлГТУ (ИСПДн УлГТУ), имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация угроз безопасности персональных данных (УБПДн), предусмотренных Базовой моделью угроз безопасности персональных данных в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008 г.

2. Защита информации при передаче ПДн в ИСПДн обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применением в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

3. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

4. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

5. При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками УлГТУ, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

6. Аутентификация пользователя осуществляется с использованием паролей. Контроль идентификации и аутентификации пользователей осуществляется уполномоченным администратором.

Для аутентификации лиц имеющих доступ к информационной системе персональных данных им выдается индивидуальный пароль. Лица, имеющие доступ к информационной системе персональных данных УлГТУ ведут журнал учета действий, совершаемых с персональными данными, в который вносятся сведения о времени начала работы с персональными данными, о времени завершения работы с персональными данными, цель обработки персональных данных.

7. Для управления идентификаторами определяется администратор ответственный за:

- создание, присвоение и уничтожение идентификаторов пользователей и устройств;
- формирование идентификатора, который однозначно идентифицирует

пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени;
- блокирование идентификатора пользователя после установленного времени неиспользования.

8. В случае использования в информационной системе УлГТУ механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:
- длина пароля не менее шести символов;
- алфавит пароля не менее 30 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут. Так же может быть установлен срок смены пароля.

9. Защита обратной связи "система - субъект доступа" в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками "*", "·" или иными знаками.

10. Идентификация и аутентификация пользователей, не являющихся работниками УлГТУ (внешних пользователей) в ИСПДн УлГТУ не допускается.

11. Для управления учетными записями пользователей определяется ответственный администратор осуществляющий:
- определение типа учетной записи внутреннего пользователя;
- объединение учетных записей в группы (при необходимости);
- верификацию пользователя проверка личности пользователя, при заведении учетной записи пользователя;
- заведение, активацию, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировку учетных записей;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе.

12. Для разграничения доступа к ПДН в ИСПДН реализуются необходимые методы, в том числе дискреционный, мандатный, ролевой или иной метод.

13. Передача информации, содержащей ПДН, в ИСПДн УлГТУ может осуществляться только по установленному маршруту (VPN).

14. УлГТУ может осуществлять передачу информации во внешние информационные системы по защищенным каналам.

15. При работе в информационной системе персональных данных УлГТУ запрещено использование виртуальной инфраструктуры, машинных носителей персональных данных, технологий беспроводного доступа, мобильных технических средств.

16. Для нейтрализации актуальных угроз информационной системе персональных данных УлГТУ используются средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации. Кроме того, должна быть реализована антивирусная защита с обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

17. Регистрация событий безопасности (в том числе сбор запись и хранение информации о событиях безопасности) осуществляется в соответствии с утверждаемой инструкцией.