Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА» (СПбГУПТД)

ПРИНЯТО

На заседании Ученого совета
СПбГУПТД,
протокол № 24 от 04 июля 2017 г.

УТВЕРЖДАЮ

Ректор СПбГУПТД

_____А. В. Демидов

ПОЛОЖЕНИЕ

ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПбГУПТД

(с изменениями и дополнениями)

Санкт-Петербург
2017

1. Общие положения

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также к информационным технологиям и техническим средствам, позволяющим осуществлять обработку таких персональных данных с использованием средств автоматизации.

Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями), Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями), Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», отраслевыми нормативными документами, уставом и определяет порядок обработки и защиты персональных данных работников и обучающихся СПбГУПТД.

2. Перечень документов, в которых содержатся сведения, составляющие персональные данные

2.1. Персональные данные работников:

– документы, предъявляемые работником при заключении трудового договора (*статья 65 Трудового кодекса РФ* (паспорт или документ, удостоверяющий личность; трудовая книжка; страховое свидетельств государственного пенсионного страхования; документы воинского учета; документ об образовании);

– документы о составе семьи работника, необходимые для предоставления гарантий, связанных с выполнением семейных обязанностей (например: свидетельство о заключении брака, свидетельство о рождении детей);

– документы о состоянии здоровья детей и других близких родственников (например: справки об инвалидности), когда с наличием таких документов связано предоставление работнику каких-либо гарантий и компенсаций;

– документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (об инвалидности, ограничении к труду в определенных условиях, донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.).

Перечень персональных данных работников представлен в приложении 1.

2.2. Персональные данные обучающихся:

– документы, предъявляемые в приемной комиссии при заполнении заявления для участия во вступительных испытаниях (паспорт или документ, удостоверяющий личность; документы воинского учета; документ об образовании);

– документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным

законодательстве (об инвалидности, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т. п.);

– медицинская справка;

– договор о внебюджетном обучении (для соответствующей категории обучающихся);

– квитанции об оплате по договору.

Перечень персональных данных обучающихся представлен в приложении 2.

3. Принципы обработки персональных данных. Условия проведения сбора и обработки персональных данных

К основным принципам обработки персональных данных можно отнести:

а) принцип законности целей и способов обработки персональных данных;

б) принцип соответствия объема и характера обрабатываемых персональных данных, способов их обработки и целям обработки персональных данных;

в) принцип достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям;

г) принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

д) принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

При обработке персональных данных должны соблюдаться, согласно *статье 86 Трудового кодекса РФ*, следующие общие требования:

1) обработка персональных данных работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации

работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет право основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ или иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работником, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

4. Работа с документами, содержащими персональные данные работника и обучающегося

Персональные данные работника содержатся в основном документе персонального учета работников – в личной карточке работника, которая заполняется сотрудником управления кадров после издания приказа о его приеме на работу и хранится в специально оборудованном шкафу.

Персональные данные обучающегося содержатся в основном документе персонального учета обучающихся – в личной карточке студента или аспиранта, которая заполняется сотрудниками директоратов, управлением аспирантуры и управления кадров после издания приказа о его зачислении на обучение и хранится в специально оборудованном шкафу.

Для уничтожения данных на бумажных носителях в подразделениях, работающих с персональными данными работников и обучающихся, должна быть установлена офисная техника – уничтожители бумаг и документов.

5. Хранение и использование персональных данных работников и обучающихся

Документы, содержащие информацию о персональных данных работника и обучающегося, хранятся на бумажных и электронных носителях в управлении кадров университета, планово-финансовом управлении, расчетном отделе управления бухгалтерского учета и финансового контроля, директоратах.

Доступ к такой информации без получения специального разрешения имеют ректор университета, главный юрисконсульт, главный бухгалтер, сотрудники управления бухгалтерского учета и финансового контроля, сотрудники управления кадров, директора институтов и сотрудники директоратов в соответствии со своими должностными обязанностями. Иные сотрудники вуза могут иметь доступ к персональным данным работников и обучающихся в случае, если они получили разрешение ректора в виде визы на служебной записке, обосновывающей необходимость ознакомления и использования персональных данных конкретного субъекта персональных данных.

Для сотрудников информационно-вычислительного центра (ИВЦ) и управления информатизации право доступа к данным в процессе настройки вычислительной техники и разработки информационных систем оговаривается в должностных инструкциях и закрепляется дополнительным трудовым соглашением.

Со сторонними работниками, сопровождающими работу информационных систем, следует заключать договоры о неразглашении персональных данных работников и обучающихся СПбГУПТД.

6. Обеспечение безопасности персональных данных при их обработке в информационных системах

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, применяемые в информационных системах.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Работа по обеспечению безопасности персональных данных при их обработке в информационных системах являются необъемлемой частью работ по созданию информационных систем.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений (с помощью систем сигнализации), в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в этих помещениях посторонних лиц.

При работе с электронными версиями документов необходимо соблюдать меры безопасности: для переноса данных использовать разрешенные носители данных, а также обеспечивать конфиденциальность проводимых работ, исключая возможность визуального считывания информации третьими лицами.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) организация учета лиц, допущенных к работе с персональными данными в информационной системе на основании служебных записок и дополнительных трудовых соглашений (учет возложить на начальника управления кадров);

з) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям,

приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании пункта 5 данного положения.

Контроль организации доступа к персональным данным возложить на начальника управления кадров, главного бухгалтера, начальника управления финансового планирования, директоров институтов, начальника отдела защиты информации.

При обнаружении нарушений порядка предоставления персональных данных начальник управления кадров незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

Для обеспечения безопасности персональных данных информационные системы, предназначенные для хранения и обработки персональных данных, должны располагаться на сервере управления кадров, управления бухгалтерского учета и финансового контроля и управления финансового планирования. Обслуживание серверов возлагается на сотрудников отдела защиты информации под общим руководством начальника ИВЦ.

7. Передача персональных данных работников и обучающихся университета

В статье 88 ТК РФ содержатся правила, которые должны соблюдаться при передаче персональных данных, так и конкретные процедуры и способы взаимодействия работников и обучающихся университета и сотрудников управления кадров, а также иных подразделений университета по передаче информации, содержащей персональные данные работников и обучающихся:

– не сообщать персональные данные работника или обучающегося третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы его жизни и здоровью, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;

– не сообщать персональные данные работника или обучающегося в коммерческих целях без его письменного согласия;

– предупредить лиц, получающих персональные данные работника или обучающегося, 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, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не

распространяется на обмен персональными данными субъектов персональных данных в порядке, установленном настоящим Кодексом и иными федеральными законами;

– осуществлять передачу персональных данных работника или обучающегося в пределах университета в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

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

– не запрашивать информацию о состоянии здоровья работника или обучающегося, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом персональных данных своих обязанностей и трудовой функции;

– передавать персональные данные работника или обучающегося представителям субъекта персональных данных в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

8. Права работников и обучающихся университета в области защиты персональных данных

Для работников эти права установлены статьей 89 Трудового кодекса РФ. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на

– полную информацию об их персональных данных и обработке этих данных;

– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

– определение своих представителей для защиты своих персональных данных;

– доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Аналогичные права имеют и обучающиеся.

9. Обязанности работников и обучающихся университета по обеспечению достоверности его персональных данных

Работники, обучающиеся и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников и обучающихся, а также об их правах и обязанностях в этой области. Работники и обучающиеся должны быть заранее предупреждены о необходимости предоставления достоверных сведений и о возможной ответственности в случае нарушения этой обязанности.

Правовой основой для установления обязанности работника и обучающегося по предоставлению достоверной информации о своих персональных данных служит положение статьи 8 ТК РФ.

10. Порядок передачи информации о работнике и обучающемся

Сотрудники управления кадров университета, управления бухгалтерского учета и финансового контроля, планово-финансового управления и директоратов, ответственные за работу с персональными данными, должны четко знать случаи, при которых они могут передать информацию о работнике и обучающемся запрашивающим лицам. К таким случаям, как правило, относят запросы о получении информации о работниках и обучающихся университета, направленные различными государственными органами.

Наиболее вероятно, что подобные запросы поступают из судебных или правоохранительных органов. Требования, поручения и запросы прокурора, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, установленных настоящим Кодексом, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

11. Ответственность за нарушение законодательства об охране персональных данных

Ответственность за нарушение законодательства об охране персональных данных может быть дисциплинарной, административной и уголовной.

К дисциплинарной ответственности может быть привлечен работник управления кадров, бухгалтерии, иного подразделения, использующего в своей работе персональные данные.

В подпункте «в» пункта 6 статьи 81 Трудового кодекса РФ предусматривается, что «разглашения охраняемой законом тайны

(государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника».

К административной ответственности могут быть привлечены как работники управления кадров и иных подразделений, так и ректор университета и организация в целом на основании статей 2.4. КоАП РФ и 13.11. КоАП РФ.

Уголовная ответственность за нарушение неприкосновенности частной жизни предусмотрена статьей 137 УК РФ.

Приложение 1

Персональные данные сотрудников

- Фамилия
- Имя
- Отчество
- Год, месяц, дата и место рождения
- Паспортные данные (серия, №, дата выдачи, кем выдан)
- Адрес, телефоны
- Семейное положение
- Социальное положение
- Сведения о детях
- Гражданство
- Образование
- Регистрационные данные документа об образовании
- Профессия
- Должность
- Место работы
- Доходы
- Документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям (об инвалидности, ... к труду.... и т.п.)
- Документы о состоянии здоровья детей и других близких родственников
- Данные о предыдущем месте работы

Приложение 2

Персональные данные обучающихся

- Фамилия
- Имя
- Отчество
- Год, месяц, дата и место рождения
- Паспортные данные (серия, №, дата выдачи, кем выдан, код подразделения)
- Домашний адрес, телефоны
- Семейное положение
- Социальное положение
- Сведения о детях
- Образование
- Регистрационные данные документа об образовании
- Стаж работы
- Национальность
- Гражданство
- Данные о родителях

ДОПОЛНИТЕЛЬНЫЕ ДАННЫЕ ДЛЯ ДОГОВОРНЫХ ОБУЧАЮЩИХСЯ:

- № договора
- На кого заключен договор
- Суммы оплат по договору
- Паспортные данные для физических лиц, на кого заключен договор
- Названия фирм/организаций, для юридических лиц
- Срок оплаты