ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

Каждое предприятие, и в особенности крупные (и не очень) промышленные предприятия собирают и обрабатывают большой объем персональных данных своих сотрудников. В эти данные входит также и информация, разглашение которой может принести вред субъекту ПДн: это и место проживания, зарплата, режим работы, семейное положение, сведения о детях и т. п. Кроме того, часть этих данных не только обрабатывается внутри предприятия, но и передается в различные государственные структуры (налоговая, пенсионный фонд, иногда ведомственные структуры, иногда силовые). Часто сотрудники предприятия занимаются покупкой билетов и бронированием гостиниц для командировочных. Иногда оформлением виз. А это тоже передача данных. Кроме того, обслуживающие сторонние организации часто получают доступ к этим базам данных при настройке программ, используемых для управления предприятием, при настройке СКУД и т. п. Есть еще один «тонкий момент» – пропуск на территорию посетителей. Особо режимные предприятия не только собирают ФИО, но требую копию паспорта, телефон, место работы и много другое.

Попробуем разобраться, насколько наше законодательство защищает субъекта ПДн и насколько «обременяет» предприятие дополнительными требованиями. С вопросами мы обратились к уже известному читателям журнала эксперту в области защиты персональных данных.

Александр Владимирович Солодянников, кандидат технических наук, доцент Государственного экономического университета, кафедры «Вычислительных систем и программирования», имеет большой опыт практических решений как генеральный директор ООО «Ассоциация специалистов по безопасности».

1. Начнем с приема на работу, оформления в отделе кадров и внесения данных в пропускную систему. Если обязательный сбор персональных данных требуется только для этих целей, то является ли предприятие «оператором» обработки персональных данных?

Предприятие, обрабатывающее персональные данные даже только своих сотрудников, является «оператором». Однако законодательство точно дает определения, когда при обработке персональных данных «оператор» вправе не уведомлять об этом уполномоченные органы:

1) обрабатываемых в соответствии с трудовым законодательством (п. 1 в ред. федерального закона от 25.07.2011 № 261-ФЗ, см. текст в предыдущей редакции);
2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных (в ред. федерального закона от 25.07.2011 № 261-ФЗ, см. текст в предыдущей редакции);
4) сделанных субъектом персональных данных общедоступными (п. 4 в ред. федерального закона от 25.07.2011 № 261-ФЗ, см. текст в предыдущей редакции);
5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;
6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка (в ред. федерального закона от 25.07.2011 № 261-ФЗ, см. текст в предыдущей редакции);
8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства (п. 9, введен федеральным законом от 25.07.2011 № 261-ФЗ).

2. Есть ли обязательные требования к работе отдела кадров по защите персональных данных?

В ОК должны обрабатываться и храниться документы двух типов:

1) документация по организации работы отдела кадров со-

держит организационно-правовую документацию, которая включает различные положения и инструкции;

2) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде, в которую входят:

а) комплексы документов, сопровождающие процесс оформления трудовых правоотношений гражданина, в т. ч. анкетирования и собеседований;

б) приказы;

в) личные дела;

г) отчетно-аналитическая база данных;

д) копии отчетов, передаваемые в государственные органы;

е) справочно-информационный банк данных по персоналу – учетно-справочный аппарат (картотеки, журналы, базы данных и др.).

При работе с документами, делами и базами данных отдела кадров должны соблюдаться следующие основополагающие принципы защиты персональных данных:

- личной ответственности работников за сохранность и конфиденциальность сведений о работе отдела и персональных данных, а также носителей этой информации;
- разбиения знания персональных данных между разными работниками отдела;
- наличия четкой разрешительной системы доступа работников отдела к документам, делам и базам данных;
- проведения регулярных проверок наличия традиционных и электронных документов, дел и баз данных у работников отдела и кадровых документов в подразделениях предприятия.

Главным моментом в защите персональных данных является четкая регламентация функций работников отдела кадров и, в соответствии с этим, регламентация принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных. Для реализации этого положения руководителем предприятия должен быть издан приказ или распоряжение о закреплении за работниками отдела определенных массивов документов, утверждена схема доступа работников отдела кадров и руководящего состава предприятия, структурных подразделений к документам отдела, введена личная ответственность перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных.

По каждой функции, выполняемой работником отдела кадров, должен быть регламентирован состав документов, дел и баз данных, с которыми этот работник имеет право работать. Не допускается, чтобы работник мог знакомиться с любыми документами и материалами отдела.

Целесообразно, в целях разграничения доступа и разбиения знания персональных данных между работниками, закрепить за разными работниками:

а) документированное оформление трудовых правоотношений (прием, перевод, увольнение и др.);

б) ведение личных дел и трудовых книжек;

в) составление и хранение приказов по личному составу и контрактов;

г) ведение справочно-информационного банка данных.

Распределение сфер деятельности может быть иным в зависимости от объема работы и штатной численности работников отдела, но разграничение обязанностей и массивов документации должно быть осуществлено в обязательном порядке.

3. Каков правильный порядок ведения личных дел и базы данных с точки зрения защиты персональных данных?

Операции по оформлению, формированию, ведению и хранению личных дел выполняются одним работником отдела кадров, который несет личную ответственность за сохранность документов в делах и доступ к делам других работников. Документы для формирования и ведения личных дел сдаются ему под роспись в передаточном журнале работником, отвечающим за процесс документирования трудовых правоотношений граждан с предприятием. Личное дело должно обязательно иметь опись документов, включенных в дело. Листы дела нумеруются в процессе формирования дела. При помещении в личное дело нового документа данные о нем первоначально вносятся в опись дела, затем листы документа нумеруются и только после этого документ подшивается. На оборотной стороне обложки личного дела может указываться список руководителей, которым дело может быть выдано для ознакомления. Здесь же подклеивается конверт для карточки учета (контрольной карточки) выдачи дела. Изменения и дополнения в персональные данные вносятся в дополнение к личному листку по учету кадров и/или личную учетную карточку формы Т-2 на основании приказов по личному составу и документов, предоставляемых сотрудниками (свидетельства о браке, диплома и т. д.). Устное заявление сотрудника не является основанием для внесения указанных изменений (кроме второстепенных сведений – изменения номера домашнего телефона, места работы близких родственников и т. п.). Все новые записи в дополнении к личному листку по учету кадров и учетных формах заверяются росписью работников отдела кадров. При переносе сведений из приказа по личному составу работник расписывается против перенесенного пункта.

В случае изъятия из личного дела документа в описи дела производится запись с указанием основания для подобного действия и нового местонахождения документа. С документа, подлежащего изъятию, снимается копия, которая подшивается на место изъятого документа. Отметка в описи и копия заверяются росписью работника отдела кадров. Замена документов в личном деле кем бы то ни было запрещается. Новые, исправленные документы помещаются вместе с ранее подшитыми.

Приказом руководителя предприятия должен быть установлен порядок выдачи или ознакомления руководящего состава с личными делами сотрудников. Личные дела могут выдаваться на рабочие места только руководителя, его заместителя по кадрам или персоналу и начальника отдела (управления) кадров. Дела выдаются под роспись в контрольной карточке. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений, включения в дело других документов или подмены документов. Передача личных дел руководителям через их секретарей или референтов не допускается. Другие должностные лица предприятия могут знакомиться с личными делами подчиненных им сотрудников. Ознакомление с делами осуществляется в помещении отдела кадров под наблюдением работника, ответственного за сохранность и ведение личных дел. Факт ознакомления фиксируется в контрольной карточке личного дела.

Сотрудник предприятия имеет право знакомиться только со своим личным делом и трудовой книжкой, учетными карточками, отражающими его персональные данные. Факт ознакомления с личным делом также фиксируется в контрольной карточке.

При организации работ необходимо выполнять следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, 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 работника, обязаны соблюдать режим секретности (конфиденциальности). Данное

положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;
- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4. Работа пропускной системы для работников предприятий. Должна ли СКУД предприятия отвечать каким-то требованиям по защите ПДн? Если для обслуживания, внесения данных, выдачи идентификаторов или настройки биометрических систем привлекаются сторонние организации – то как происходит защита ПДн? Если обслуживающие организации используют удаленный доступ, то какие требования возникают?

Если в составе СКУД используются средства автоматизации (АРМ, ЭВМ), то подлежат защите в соответствии с требованиями ФЗ 152 и подзаконных актов. Отдельно остановимся на специфике биометрических систем. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

Исключение – обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, оперативно-розыскной деятельности, государственной службе, уголовно-исполнительным законодательством, законодательством о порядке выезда и въезда в Российскую Федерацию (в ред. федерального закона от 25.11.2009 № 266-ФЗ).

Для проектирования, наладки и обслуживания СКУД обычно привлекаются сторонние организации. При привлечении третьих лиц к ПДн своих сотрудников в договоре с третьим лицом необходимо прописывать ответственность за обеспечение защиты. А в соглашении сотрудника необходимо конкретно прописывать, каким третьим лицам он (сотрудник) разрешает передавать ПДн. Если обслуживающая организация использует удаленный доступ, канал передачи должен защищаться.

5. Пропуск посетителей – насколько законны требования предприятий по сбору у посетителей полных ПДн, включающих копию паспорта (права), контактные данные и т. п. Должно ли предприятие получать согласие на обработку ПДн в обязательном порядке? Если эти данные вводятся в общую систему СКУД, то означает ли это, что предприятие автоматически становится «оператором» и возникают требования по защите ПДн?

Сбор у посетителей полных ПДн не является необходимостью, влияющей на функционирование предприятия. Закон не предусматривает обязательный сбор ПДн. Поэтому предприятие, осуществляющее сбор ПДн, обязано получать согласие у посетителей на их обработку. При обработке ПДн посетителей и для включения в базу данных СКУД с применением средств автоматизации предприятие становиться «оператором» обработки ПДн. Соответственно, обязано реализовывать требования по защите. Но при этом не обязано уведомлять контролирующий орган.

6. Если ПДн сотрудника предприятия передаются «третьим лицам», например, заказ билетов и гостиниц от имени предприятия или передача данных для оформления пропуска для командировки на предприятие партнера, или передача сведений в ведомственные или силовые структуры по требованию режима предприятия – становится ли предприятие «оператором» и какие требования возникают к системам обработки и передачи ПДн и к сотрудникам предприятия, включенным в этот вопрос. Может ли сотрудник предприятия, осуществляющий передачу данных, пользоваться личной электронной почтой для каких-то целей?

При привлечении третьих лиц к ПДн своих сотрудников в договоре с третьим лицом необходимо прописывать ответственность за обеспечение защиты. А в соглашении сотрудника необходимо конкретно прописывать, каким третьим лицам он (сотрудник) их разрешает передавать. При использовании удаленного доступа канал передачи должен защищаться.

При передаче ПДн третьим лицам предприятие становится «оператором» обработки ПДн. Но при этом не обязано уведомлять контролирующий орган. Сотрудники, задействованные в обработке ПДн (хранении, передаче), должны пройти инструктаж по правилам обеспечения защиты ПДн. А работодатель – организовать данный инструктаж. Пользоваться личной почтой для передачи ПДн другого сотрудника можно только с его письменного разрешения.

7. Требуется ли отдельное разрешение сотрудника предприятия на обработку его ПДн, даже если предприятие по нормам не является «оператором», но фактически эти данные собирает, обрабатывает и передает? Достаточно ли прописать это разрешение в трудовом договоре?

Согласие сотрудника на обработку ПДн требуется при приеме на работу, даже если предприятие не является «оператором». Согласие подписывается в двух экземплярах при подписании трудового договора. Один экземпляр хранится в личном деле.

8. Если предприятие все-таки является «оператором» – то какие нормативные акты регулируют применение средств по защите персональных данных? Есть ли список лицензированных для этих целей средств и ПО, и где он опубликован? Накладываются ли какие-то требования, связанные с защитой ПДн, на оборудование и ПО при закупках?

Средства защиты ПДн (СрЗИ) выбираются в процессе реализации мероприятий по защите. Существует реестр сертифицированных ФСТЭК СрЗИ, размещенный на сайте ФСТЭК России (fstec.ru). На оборудование и ПО никаких дополнительных требований не накладывается. При обработке ПДн должны быть реализованы мероприятия, включающие в себя разработку документации, внедрение технических и программных средств, контроль эффективности.