Персональные данные: оптимальные решения

В.В. Алехин,
руководитель департамента защиты информации ГК "Контек"

Проблемы защиты персональных данных весьма актуальны для организаций ЖКХ.

Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" существенно изменен 25 июля 2011 г. В ближайший год ожидается появление ряда новых подзаконных актов.

Персональные данные в ЖКХ

Разночтения в нормативных документах обусловлены различным толкованием основных понятий. Уточним их.

К **персональным данным** (общепринятое сокращение – ПДн) относится *любая информация* о конкретном человеке (физическом лице). Обработка персональных данных – это *любые действия*, производимые с такой информацией (включая хранение и передачу). И в том случае, если персональные данные только хранятся, и в том, если только собираются и передаются, имеет место обработка персональных данных и соответственно применимо законодательство о персональных данных.

Информационная система персональных данных (общепринятое сокращение – ИСПДн) – это технические средства (компьютеры), на которых установлена база персональных данных и программное обеспечение, которое работает с этой базой. Для ЖКХ специфичны следующие виды ИСПДн: расчет квартплаты, паспортный стол, диспетчерская служба.

В каждой ИСПДн ведется обработка персональных данных соответствующих субъектов: собственников и нанимателей, граждан, зарегистрированных по месту жительства и месту пребывания, и заявителей (граждан, оставивших заявку диспетчеру).

Субъекту персональных данных противопоставляется *оператор* – лицо, которое организует и (или) осуществляет обработку персональных данных и при этом определяет цели обработки, состав ПДн и конкретные действия по обработке. Оператор может и не осуществлять обработку ПДн, а полностью *поручить* ее другим лицам. Здесь можно провести аналогию с генеральным подрядчиком (оператором) и субподрядчиком (осуществляющим обработку по поручению оператора).

Защита прав субъектов ПДн. Закон допускает обработку персональных данных лишь в определенных случаях. К организациям сферы ЖКХ применимы следующие:

- обработка с согласия субъекта персональных данных (физического лица);
- по договору с субъектом;
- на основании закона.

Если оператор поручает обработку ПДн другим организациям (обработчикам), то он должен получить согласие субъектов на обработку их ПДн в этих организациях. При этом оператор несет ответственность за обработку ПДн перед субъектом, а обработчики – перед оператором. В остальном операторы и обработчики должны выполнять одни и те же требования.

Закон также устанавливает права субъектов на запросы к операторам и обязанности операторов при ответе на них. Этот вопрос крайне важен, поскольку невыполнение этих простых обязанностей может повлечь за собой внеплановую проверку со стороны уполномоченного органа по защите прав субъектов (Роскомнадзора).

Защита персональных данных. Помимо решения первостепенных правовых вопросов необходимо обеспечить защиту собственно персональных данных, хранящихся в базах. Нормативные документы, регламентирующие эти вопросы в настоящее время, подлежат переработке. Однако общие моменты можно отметить.

Прежде всего, меры по защите информации можно разделить на организационные и технические. Большая часть затрат на технические меры идет на защиту персональных данных.

Обязательным требованием по технической защите является защита от несанкционированного доступа (НСД), которая подразумевает идентификацию и проверку подлинности пользователей (например, по ключу), разграничение доступа пользователей к различным информационным ресурсам, а также регистрацию действий пользователей. Защита от НСД должна быть установлена на любом компьютере, имеющем доступ к базе персональных данных.

В случае если компьютеры, имеющие доступ к персональным данным, подключены к сети связи общего доступа (как правило, Интернету), необходимо установить межсетевой экран (firewall) на компьютере или шлюзе. Самое простое и недорогое решение – отключить компьютеры, имеющие доступ к персональным данным, от сетей связи общего доступа. Но это не всегда возможно и целесообразно.

При передаче персональных данных по открытым каналам связи необходимо шифрование передаваемых сообщений. По закону шифровальные средства должны быть сертифицированы в системе сертификации ФСБ России.

Спектр проблем по защите персональных данных широк: начиная от квитанций на оплату коммунальных услуг в открытых почтовых ящиках и списков должников в подъездах с указанием сумм долга и заканчивая передачей реестров платежей по открытым каналам связи (например, по электронной почте), слабыми паролями или вообще отсутствием таковых.

Решения для организаций ЖКХ

Для целей представления оптимальных решений по защите персональных данных рассмотрены следующие варианты:

- ТСЖ, ЖСК, небольшая УК (прием населения и обработка ПДн в одном здании);
- крупная УК (прием населения и обработка ПДн в нескольких зданиях);
- работа с информационно-расчетными центрами (ИРЦ);
- работа с другими организациями (например, ресурсоснабжающими, банками, платежными системами).

Организации ЖКХ различаются по многим параметрам: организационно-правовой форме, видам деятельности, размеру, структуре и т. п.

Малые организации ЖКХ. Если ТСЖ, ЖСК, УК самостоятельно управляет жилым фондом, то вопросы защиты прав субъектов персональных данных решаются достаточно просто. У них имеются законные основания на обработку персональных данных. Так, расчет квартплаты производится по договорам управления с собственниками жилых помещений, регистрация и снятие с регистрационного учета – по Закону РФ от 25.06.1993 № 5242-I, а работа диспетчера – с согласия заявителя (он сообщает какие-либо данные о себе, следовательно, дает согласие на их обработку).

Так же просто решаются и вопросы технической защиты информации. Для организаций, офис которых полностью расположен в одном здании, тем не менее актуальны автоматизация и информатизация. Как правило, такие информационные системы представляют собой автономный компьютер или локальную сеть без выхода в Интернет. Тогда технические меры сводятся к установке на каждом компьютере средств защиты информации от несанкционированного доступа, что по цене сопоставимо с покупкой нового монитора для каждого компьютера.

Крупные управляющие компании. Рано или поздно руководство большой управляющей компании принимает решение соединить удаленные филиалы в одну распределенную корпоративную сеть. Для этого каждый филиал подключается к Интернету, и таким образом осуществляется консолидация баз персональных данных (или доступ к централизованной базе). В этом случае нормативы по защите информации требуют установки межсетевых экранов и шифровальных средств, что приводит к дополнительным затратам.

Работа с ИРЦ. Концепция ИРЦ как единого центра информатизации достаточно привлекательна для многих участников отрасли. Далее деятельность ИРЦ будет рассмотрена с точки зрения правовой и технической защиты персональных данных.

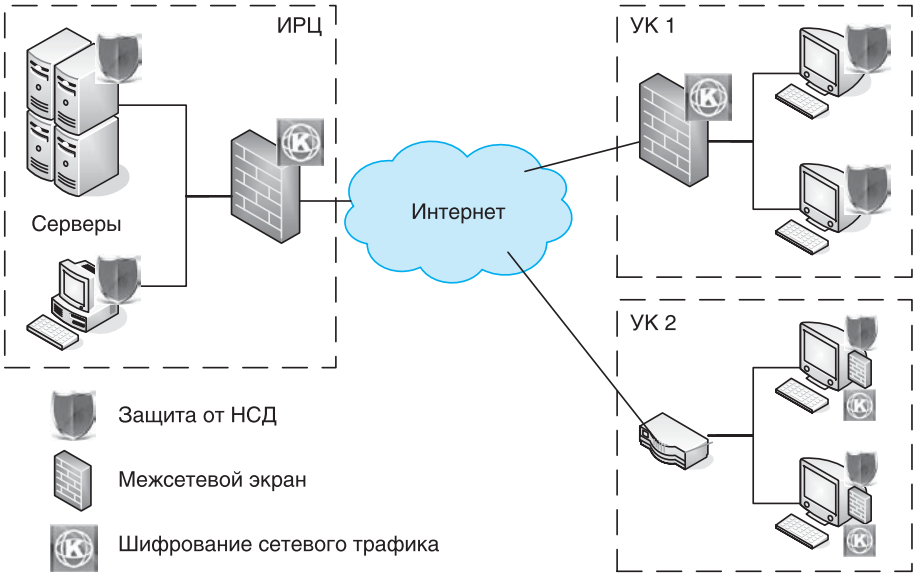
Управляющая компания (ТСЖ, ЖСК), как правило, заключает с ИРЦ договор на начисление платежей. По этому договору УК фактически поручает ИРЦ обработку ПДн. Кстати, встречающиеся на практике договоры чаще всего не удовлетворяют требованиям закона к содержанию такого поручения. Таким образом, УК (ТСЖ, ЖСК) является оператором, а ИРЦ – лицом, осуществляющим обработку персональных данных по поручению оператора.

Нередки случаи, когда УК практически полностью передают ИРЦ свои функции по обработке персональных данных. Однако это не снимает с УК обязанности оператора ПДн. В частности, дополнительной обязанностью оператора (УК) в случае обработки ПДн в другой организации (ИРЦ) является получение дополнительного согласия субъекта ПДн на обработку его данных в этой конкретной организации.

В случае если обработка ведется на основании договора или получения согласия (расчет квартплаты и диспетчерская служба), получить такое дополнительное согласие нетрудно (дополнить договор или существующее согласие). Сложнее дела обстоят, когда обработка ведется для достижения целей закона (паспортный стол), в этом случае приходится получать согласие непосредственным образом. Это осложняется еще и тем, что такое согласие нужно получить у каждого жителя города, обслуживаемого ИРЦ.

Информационные системы, работающие в ИРЦ, как правило, являются распределенными. Поэтому необходимо обеспечить не только защиту от несанкционированного доступа, но и межсетевое экранирование и шифрование сообщений, передаваемых по сетям связи. Возникает спорный вопрос: за чей счет должна быть оплачена защита – ИРЦ или УК? Разумным представляется следующее решение: организация, на территории которой располагаются информационные системы, оплачивает их защиту. Наглядно это можно изобразить на рисунке: ИРЦ оплачивает те средства защиты, которые расположены на его территории, а УК – которые расположены на их территории (рисунок).

Обязанности оператора ПДн требуют от УК получения дополнительного согласия субъекта ПДн на обработку его данных конкретным ИРЦ.



Защиту информационных систем оплачивает та организация, на чьей территории они расположены

Работа с другими организациями. Управляющие организации взаимодействуют со множеством других организаций, которые в той или иной степени связаны с обработкой персональных данных. К этой категории относятся ресурсоснабжающие организации (РСО), банки и платежные системы.

Обработка ПДн в РСО (поставщики электроэнергии, воды и т. п.) зависит от способа управления многоквартирным домом. В случае непосредственного управления собственники жилых помещений заключают с РСО договоры на предоставление соответствующих услуг, и согласно этому договору РСО получают право на обработку персональных данных собственников. В случае управления с помощью УК (ТСЖ, ЖСК) такие договоры заключаются соответственно с УК (ТСЖ, ЖСК), и для предоставления ПДн в РСО уже необходимо согласие каждого субъекта, что весьма накладно.

РСО может производить обработку ПДн в целях проверки количества проживающих (если начисление производится по нормативу) либо если такая схема работы традиционно сложилась в конкретном городе. В большинстве случаев можно отказаться от обработки ПДн в РСО, что сэкономит и время, и деньги участников договорных отношений.

Отказ РСО от обработки ПДн сэкономит время и деньги участников договорных отношений.

Взаимодействие с банками и платежными системами позволяет облегчить (для плательщиков) процесс сбора платы за коммунальные услуги. При этом, как правило, производится обмен реестрами платежей, которые содержат персональные данные. Лучшим решением в данном случае является обезличивание этих персональных данных. Например, для оплаты коммунальных услуг на квартиру достаточно знать адрес этой квартиры, а Ф.И.О. собственника – это уже избыточная информация. Разумеется, передача таких реестров должна производиться по защищенным каналам связи с использованием сертифицированных средств шифрования.

Типовые решения

Реализация технических мер – наиболее сложный этап защиты персональных данных (к тому же лицензируемый). Правовые и организационные меры в большей степени типовые и заключаются в принятии определенного набора локальных регламентов, действующих в организации. Такие регламенты важны, поскольку документы – это первое, что проверяется в рамках любого государственного контроля.

Существуют шаблоны таких документов: бесплатные и платные, общие и отраслевые, устаревшие и актуальные. В сети Интернет пока присутствует лишь один комплект документов по защите персональных данных, а именно для УК, ТСЖ, ЖСК. Помимо этого,

разработчики обещают поддерживать этот комплект в актуальном состоянии на сайте: *www.gkhpd.ru*.

Вопрос защиты персональных данных в ИРЦ не менее важен, чем в малых предприятиях ЖКХ. Так, в 2008 г. в Омске мировым судом была фактически блокирована деятельность ИРЦ из-за того, что УК неправомерно передавали ПДн в ИРЦ, также подобного рода инцидент имел место на Дальнем Востоке. По этой причине среди ИРЦ больше осведомленных организаций и велика доля организаций, уже ведущих свою деятельность в соответствии с требованиями законодательства о персональных данных, нежели среди УК. Между тем типовых решений по защите ПДн для ИРЦ не существует ввиду относительной сложности такого рода организаций. Поэтому защитой ПДн в ИРЦ занимаются в основном специализированные компании, имеющие лицензии на деятельность, связанную с защитой конфиденциальной информации.

В данной статье были кратко рассмотрены типовые решения по защите персональных данных для различных организаций отрасли ЖКХ. Налицо следующий факт: чем более привлекательна информационная инфраструктура, тем дороже обходится ее защита. Организационная и техническая стороны вопроса (конкретные требования по защите информации) будут уточняться по мере разработки соответствующих нормативных актов в 2012 г.

Правовая сторона вопроса, напротив, достаточно устоялась, и организациям, связанным с обработкой персональных данных, необходимо в срочном порядке приступить к выполнению основных требований по защите прав субъектов персональных данных: сформулировать цели и основания обработки персональных данных, собрать согласие на обработку персональных данных, назначить ответственного за организацию обработки персональных данных и т. п.

Чем более привлекательна информационная инфраструктура, тем дороже обходится ее защита.