Е. И. Гончаров

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ОБМЕНА МЕЖДУ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В последние годы обозначилась тенденция к глобализации и интеграции информационных систем персональных данных (ИСПД). Одним из ярких примеров является пилотный проект «Универсальная социальная карта», цель которого — создание единой общероссийской социальной карты. С ее помощью любой льготник сможет воспользоваться не только всеми положенными ему социальными льготами, но и банковскими, транспортными и другими услугами. Также предусматривается возможность применения данной карты в качестве электронного паспорта гражданина РФ.

С помощью карты предоставляется доступ к услугам различных государственных организаций и коммерческих предприятий, а значит, встает вопрос организации и защиты обмена данными как с общей (центральной) базой данных, так и между контрагентами. Принципиальная схема взаимодействия представлена на рис. 1. В связи с тем, что для многих операций предоставления услуг необходимы не только обезличенные данные (номер кристалла карты), но и персональные данные держателя карты (ПДДК), такие ИСПД и обмен ими должны быть защищены согласно требованиями ФЗ «О персональных данных».

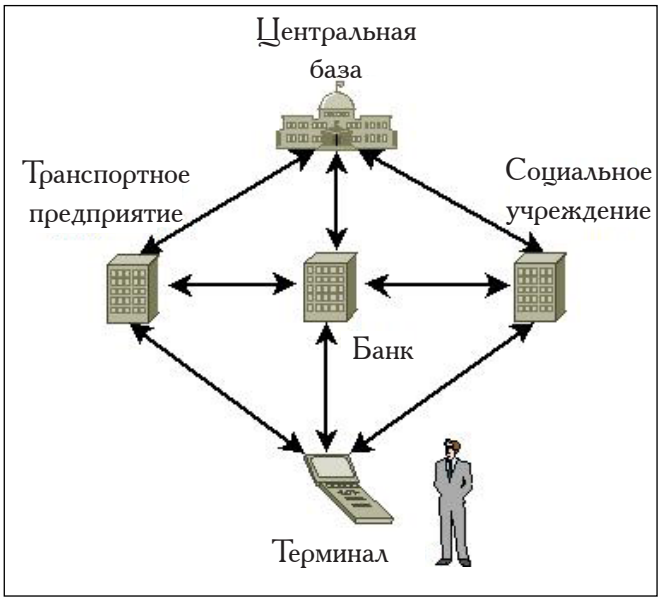

Рис. 1. Принципиальная схема взаимодействия в проекте «Универсальная социальная карта»

Разумно предположить, что участниками данного проекта будут ИСПД различного класса. Это следует даже из критериев, положенных в основу классификации ИСПД [1]:

1. по набору персональных данных — имя, фамилия, национальность и т. п.,

2. по количеству персональных данных.

Таким образом, например, филиал какого-либо социального учреждения в малонаселенном районе может быть отнесен к классу К2, а филиал этого же социального учреждения в мегаполисе — к классу К1, и все они должны взаимодействовать с центральной базой данных, очевидно, класса К1.

Так как во взаимодействии участвуют информационные системы, отнесенные к различным классам ИСПД, то необходимо гарантировать, что между этими системами не происходит

интеграции. В противном случае всем интегрированным системам автоматически присваивается, как минимум, класс системы, имеющей максимальный класс (см. рис. 2).

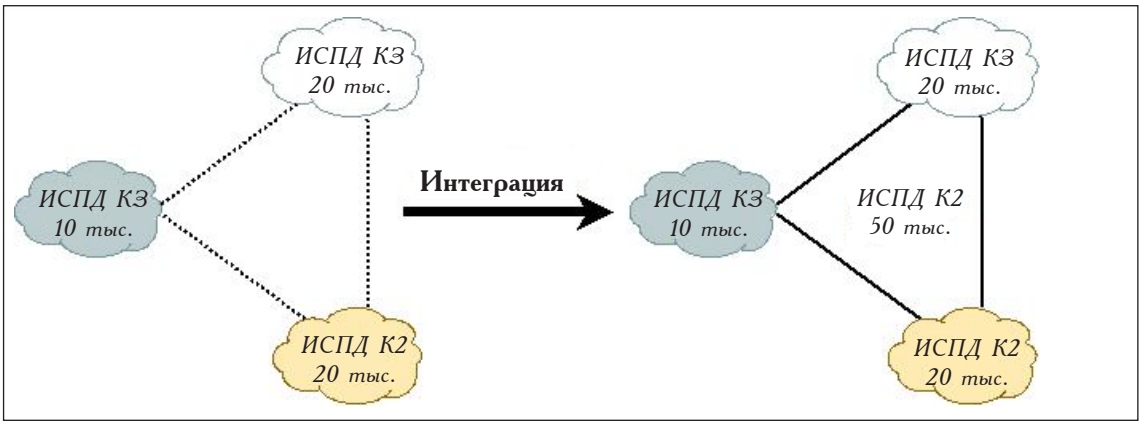

Рис. 2. Интеграция ИСПД

Т. е. при организации взаимодействия между ИСПД классов К2 и К3, результатом которого становится интеграция между ними, все эти системы автоматически причисляются к классу К2. Если же суммарное количество персональных данных превысит 100 тысяч записей [1] — к классу К1 (см. рис. 3).

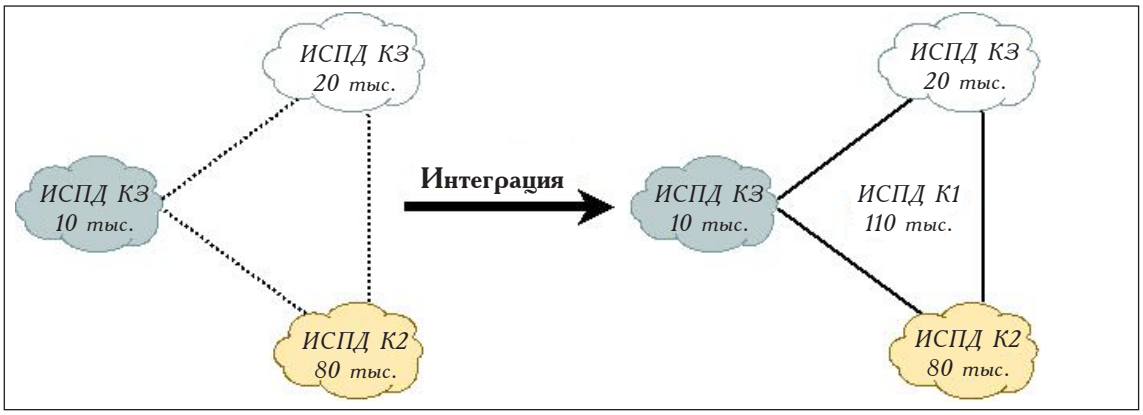

Рис. 3. Интеграция ИСПД с повышением класса

Кроме того, даже в случае, когда интеграции нет, остается вопрос безопасного доступа к ПДДК из систем с низким классом (так как системы класса К1, как правило, изначально достаточно защищены). Например, уже упоминавшийся ранее филиал социального учреждения в малонаселенном районе имеет доступ ко всей федеральной базе льготников и их ПДДК, так как по замыслу проекта универсальной карты она не имеет ограничения по регионам использования и может использоваться на всей территории РФ. Следовательно, от добросовестности немногочисленного штата сотрудников этого учреждения будет зависеть безопасность персональных данных федерального масштаба. В то же время защищать такие филиалы по требованиям к ИСПД класса К1 далеко не всегда экономически разумно.

Полностью решить проблемы интеграции и безопасности удаленного доступа к ПДДК традиционными средствами защиты информации, такими как межсетевые экраны, средства контроля доступа и средства криптографической защиты, невозможно, так как они не могут учитывать ни объем, ни категорию передаваемых персональных данных, которые лежат в основе классификации ИСПД. В качестве решения предлагается использовать некоторый программно-аппаратный комплекс — обозначим его как «информационный шлюз» или «посредник». Информационный шлюз устанавливается перед отделяемой им ИСПД, и весь информационный

обмен проходит только при его участии. Если проводить аналогию с сетевой безопасностью, то информационный шлюз напоминает межсетевой экран (МЭ) с технологией stateful inspection (анализ сетевых пакетов по всем уровням модели OSI и отслеживание состояния соединений). Разница между ними заключается в уровнях и данных, которыми оперируют эти устройства:

- межсетевой экран проверяет отправителя/получателя сетевых пакетов, корректность самих пакетов с точки зрения сетевых протоколов и сверяет их с сигнатурами атак. МЭ никогда не является инициатором информационного потока;
- информационный шлюз работает на более высоком уровне — проверяет отправителя/получателя, легальность и целостность передаваемых данных с помощью набора правил или по шаблону, количество передаваемых данных и выполнение иных правил, необходимых для организации безопасного обмена. Информационный шлюз является инициатором информационного обмена, т. е. только его настройкой определяются информационные потоки из/в отделяемую ИС.

Таким образом, информационный шлюз представляет собой ИСПД-посредника, передающего персональные данные строго определенной категории от фиксированного отправителя фиксированному получателю, при этом контролируя целостность данных и их объем в процессе как обработки, так и хранения. Необходимость контролировать объем данных на самом шлюзе вытекает из критериев классификации информационных систем обработки персональных данных [1]:

- категория персональных данных, участвующих в обработке;
- объем одновременно обрабатываемых и хранимых данных.

В процессе обмена информационный шлюз выполняет следующие операции:

1. устанавливает соединение с источником данных, проверяя его подлинность;
2. устанавливает соединение с получателем данных, также проверяя его подлинность;
3. получает заданное количество данных и проверяет их целостность и количество согласно настроенным на шлюзе критериям;
4. передает данные от источника получателю;
5. очищает оперативную память и удаляет с себя все файлы, хранившие переданные данные и производные.

На рис. 4 показано размещение информационного шлюза относительно взаимодействующих ИС и направление сетевых соединений.

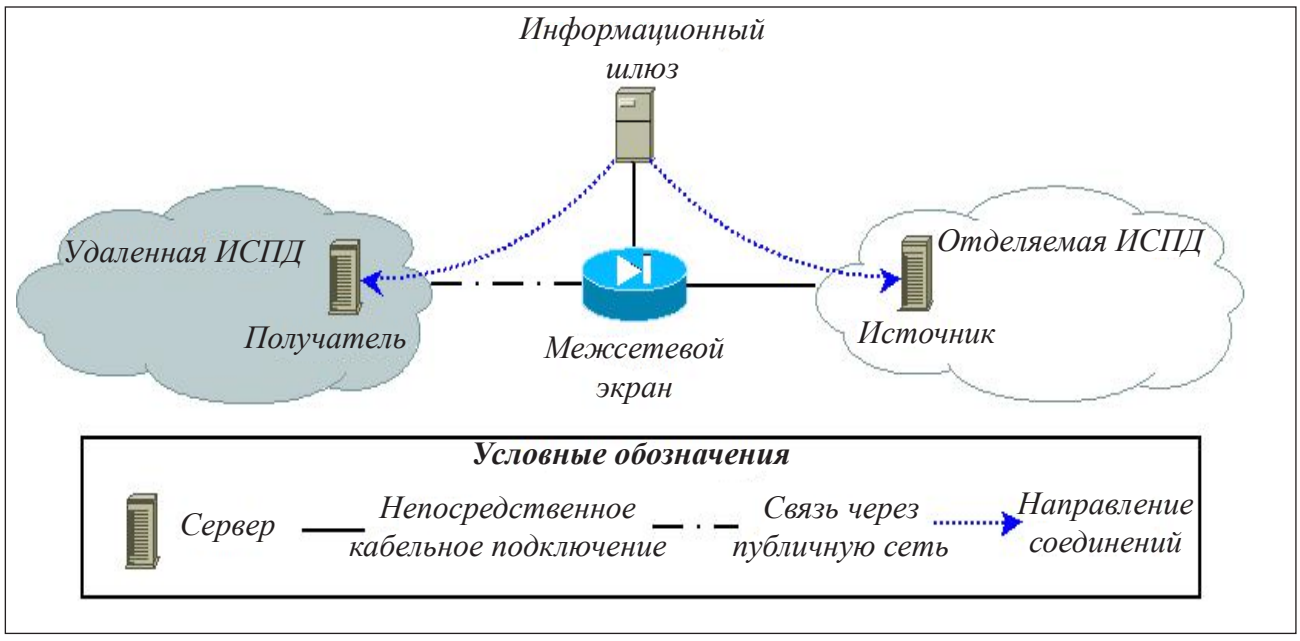

Рис. 4. Размещение информационного шлюза по отношению к ИСПД

Отделение информационного шлюза с помощью МЭ от ИСПД, с которыми организуется обмен, необходимо вследствие того, что информационный шлюз сам, по сути, является обособленной ИСПД, которая, благодаря такому обособлению, и должна гарантировать отсутствие интеграции между взаимодействующими системами, а значит, в отношении него, как и любой ИСПД, должны выполняться все требования соответствующих руководящих документов. Класс необходимого МЭ зависит от класса ИСПД, к которому будет отнесен информационный шлюз.

Для того чтобы шлюз сам не был интегрирован, участвуя во взаимодействии ИС, и соответствовал требованиям руководящих документов, необходимо выполнение таких требований, как:

- использование коммуникационного ПО, которое определяет и контролирует категорию передаваемых персональных данных, их объем, целостность;
- обеспечение закрытой программной среды шлюза, которая позволила бы гарантировать целостность ПО и настроек шлюза;
- выделение сетевого сегмента шлюза за межсетевой экран соответствующего класса защищенности. Класс межсетевого экрана не может быть ниже класса, необходимого для защиты сети ИСПД того класса, которому принадлежит шлюз;
- ограничение на межсетевом экране сетевых сервисов и узлов, которые доступны шлюзу, только списком конкретных сервисов и узлов, необходимых для информационного обмена;
- отключение сетевого доступа к шлюзу извне, как всем пользователям ИС, так и обслуживающему персоналу — шлюз должен являться единственным инициатором сетевого взаимодействия.

При условии выполнения всех перечисленных требований:

- можно гарантировать отсутствие интеграции между шлюзом и отделяемыми им ИС;
- информационный шлюз может быть отнесен к более низкому классу ИСПД, что значительно расширяет круг возможных для использования в его реализации программно-аппаратных средств и снижает затраты.

Рассмотренная схема была реализована в одной из крупных ИСПД для взаимодействия с другими ИС и успешно прошла государственную сертификацию.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных».