ЮРИСПРУДЕНЦИЯ

Добрякова Галина Эдуардовна
канд. юрид. наук, преподаватель
Московский государственный машиностроительный университет
г. Москва

СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ СИСТЕМЫ-ПОСРЕДНИКА

Аннотация*: в статье рассмотрены проблемы соблюдения требований информационной безопасности в деятельности системы посредника. Рассмотрены вопросы обеспечения безопасности персональных данных. Сделан вывод о необходимости аппаратной обработки данных либо использования идентификатора типа электронного паспорта.*

Ключевые слова*: информационная безопасность, система-посредник, безопасность персональных данных.*

Анализ соблюдения требований информационной безопасности в деятельности системы-посредника следует начать с определения системы-посредника.

Система-посредник – информационная система (АСУ), обеспечивающая осуществление согласованных действий пользователей, направленных на заключение и исполнение сделки.

Основной особенностью системы посредника является наличие программно-аппаратной технологии, позволяющей осуществлять пользовательское взаимодействие без участия человека.

Система-посредник может содержать элементы экспертной системы, возможность доступа в базу персональных данных в отношении пользователей системы, а также технологию взаимодействия с массивами данных при проведении авторизации пользователя и объекта, также система может выступать гарантом и арбитром сделки, и агентом для обеспечения платежей.

Взаимодействие с системой-посредником осуществляется посредством информационно-телекоммуникационных систем, поэтому система-посредник также является информационным посредником и оператором связи, поскольку получает и передает телекоммуникационные сигналы пользователей.

В соответствии с доктринальным определением, информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий.

Прежде, чем переходить к анализу мер, необходимо сказать несколько слов об «уязвимых точках» системы-посредника с точки зрения информационной безопасности. Если разбить на блоки, то получится, что уязвимыми точками обладают следующие блоки:

Идентификация – во время этой процедуры пользователь сообщает персональные данные, в будущем, эту проблему можно решить через идентификацию по УЭК, электронный паспорт нового поколения либо иной глобальный идентификатор – в этом случае в самой системе не будут храниться и обрабатываться персональные данные.

Аутентификации – во время этой операции сторона сделки вводит пароль, который знает для доступа в систему и второй пароль, который приходит на мобильное устройство стороны сделки. Возможен захват информации (маловероятно технически), но более вероятным риском является утрата Пользователем пароля и мобильного устройства, что потребует незамедлительной блокировки.

Идентификация объекта сделки – пользователь может ввести объект, изъятый из оборота либо ограниченный в обороте. Технически защитить от этого систему невозможно, поскольку Пользователи вводят объекты сами. Разумеется, объект не пройдет авторизацию, но для ряда объектов этого не требуется. В данном случае сделка будет недействительной (порок объекта) и не будет обладать правовой защитой, поэтому стороны по сделки не получат правовую защиту, а все полученное по сделке подлежит взысканию в доход государства, поэтому трудно представить такую ситуацию для пользователей системы-посредника, где гарантии сделки являются основной задачей.

Согласование сделки – поскольку ряд условий можно прописать вручную, а модерация администратором не является обязательной, возможна ситуация, когда сторона пропишет кабальные условия сделки, а вторая с ними согласится. В системе-посреднике планируется решить данную задачу за счет платной модерации условий договора.

Взлом системы – один из рисков информационной безопасности, но система-посредник не представляет интереса с точки зрения взлома системы, поскольку базы данных хранятся на различных серверах и непосредственно в системе (в сети Интернет) не представлены. Оперирование осуществляется ID номерами пользователей и предметов, поэтому единственное, что может получить злоумышленник при взломе системы – это набор непонятных номеров и договоров с непонятными номерами, а для проведения сличения и идентификации номеров потребуется доступ к каждому отдельному серверу, что представляется затруднительным, поскольку осуществляется только в момент сделки.

Копирование баз данных – является наиболее существенным риском, но, к сожалению, технической защиты предусмотреть невозможно. В доступе на настоящий момент находятся даже базы Росреестра, ФМС и паспортные данные пользователей, хотя их технологии защиты разрабатывались годами.

Как следует из приведенного перечня, практически все, кроме персональных данных не несет в себе угроз информационной безопасности. Особое внимание необходимо уделить именно защите персональных данных.

С правовой точки зрения, защита персональных данных будет осуществляться путем соблюдения требований законодательство относительно процедуры получения, хранения и обработки персональных данных.

Технологически же в системе-посреднике в качестве мер по защите персональных данных, можно предложить автоматическую обработку и сопоставление программно-аппаратными средствами без участия человека. Данная обработка данных программно-аппаратными средствами благотворно скажется как на скорости проведения процедуры аутентификации, так и на безопасности персональных данных. Следовательно, путем предоставления автоматизированного

доступа к регистрам, содержащим персональные данные, решится вопрос о хранении и использовании, а в равной мере согласия на использование персональных данных.

Что касается изъятия персональных данных, то рассуждая о правах человека, не следует забывать о мнении профессора Голосковова А.В., который точно сформулировал опасения при движении по пути тотальной защиты персональных данных: «как мы полагаем, модернизация концепции прав человека должна проявиться в том, что, заботясь о защите персональных данных и частной жизни, мы должны извлекать уроки из того, что террористы пока могут ходить по улицам российских городов и долго готовиться к террористическим актам. Технические проблемы дистанционной идентификации будут стоить, конечно, дорого, но, если не использовать эти возможности, нас могут ждать новые подобные бедствия, и, в конечном итоге, нарушение прав законопослушных граждан».

Как сторона по сделке, добросовестный клиент системы-посредника, разумеется, желает, чтобы данные его контрагента были подлинными, а сделка носила бесспорный характер, но возможность отзыва персональных данных фактически лишает его этой возможности. Недобросовестный контрагент вправе после начала цикла, – поскольку он вправе это сделать в любое время в соответствии с действующим законодательством, – прекратить доступ к персональным данным, что впоследствии даст ему возможность говорить о недействительности сделки.

Список литературы

1. Голосков А.В. «Модернизация российского права: теоретико-информационный аспект» диссертация на соискание ученой степени доктора юридических наук. 2006. с. 347.

2. Полякова Татьяна Анатольевна «Правовое обеспечение информационной безопасности при построении информационного общества в России диссертация на соискание ученой степени доктора юридических наук, 2008 г. с. 326–327.