

Защита персональных данных в кредитно-финансовых учреждениях



Михаил
Емельяников
Директор
по развитию
бизнеса компании
«Информзащита»

Вопросы о том, являются ли операторами персональных данных банки, бюро кредитных историй, коллекторские агентства, относятся ли автоматизированные банковские системы (АБС) и системы дистанционного банковского обслуживания (ДБО) к информационным системам персональных данных (ИСПДн), нуждаются ли они в аттестации или сертификации и т. п., уже не стоят. Ответы на них получены и от представителей регуляторов в области персональных данных (ФСБ, ФСТЭК, Росвязькомнадзор), и от банковского сообщества. Проблемы перешли в практическую плоскость — что и как нужно делать, чтобы при работе с персональными данными выполнялись положения закона. До «экзаменов» совсем недолго — к 1 января 2010 г. обработка данных в ИСПДн должна быть приведена в соответствие с требованиями законодательства.

Масштабы и границы

Уже сейчас ясно, что мероприятия по обеспечению безопасности обработки персональных данных являются технически сложными, требуют высокой квалификации исполнителей, специальных знаний, глубокого понимания функциональности как приложений, обрабатывающих персональные данные, так и средств защиты информации. Именно поэтому нормативные документы регуляторов предусматривают лицензирование деятельности

операторов персональных данных по технической защите конфиденциальной информации. Выходом для банковских учреждений, которые по тем или иным причинам не могут или не хотят получать лицензию, является заключение договора со специализированной организацией-лицензиатом на аутсорсинг услуг по технической защите персональных данных.

Независимо от того, кто будет выполнять работы по обеспечению безопасности обработки персональных данных,

первые шаги оператора достаточно очевидны. Необходимо (1) выявить все информационные системы, обрабатывающие персональные данные (ИСПДн), (2) классифицировать все выявленные ИСПДн и (3) сформировать и актуализировать для каждой из них или групп однотипных систем модель угроз.

При этом важно понимать, что определение границ ИСПДн и их классификация — задачи неформальные, требующие понимания бизнес-процессов. Ключевыми моментами на этапе сбора и анализа исходных данных по ИСПДн являются определение целей обработки персональных данных и формирование перечня ПДн (определение состава сведений, отнесенных к такой категории).

Приведем два примера.

Первый пример. Большинство крупных организаций, и банки здесь — не исключение, имеют внутренние корпоративные порталы, содержащие среди прочего и справочную систему, в которой размещены сведения о сотрудниках с указанием их фамилии, имени, отчества, должности, номера служебного телефона и кабинета, адреса электронной почты, в некоторых случаях — и фотографии. При определении категории подобных персональных данных по методике совместного приказа ФСТЭК, ФСБ и Мининформсвязи России от 13 февраля 2008 г.

№ 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» необходимо исходить из цели обработки данных — идентификация сотрудников для установления контакта с ними (категория 3), а при оценке коэффициента, характеризующего количество обрабатываемых записей (ХНПД), в качестве параметра выбрать «персональные данные субъектов персональных данных в пределах конкретной организации». В этом случае справочная система будет относиться к классу 3 (К3) типовых ИСПДн, даже если в организации работает более 1000 сотрудников.

Второй пример. При формировании перечня персональных данных для сегмента АБС, связанного с ведением кредитной истории клиента, перечень обрабатываемых персональных данных можно определить на основании Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях». Тогда к персональным данным именно в этой ИСПДн будут относиться следующие сведения о заемщике:

- фамилия, имя, отчество;
- дата и место рождения;
- данные паспорта или иного документа, удостоверяющего личность (номер, дата и место выдачи, наименование выдавшего его органа);
- ИНН;
- страховой номер индивидуального лицевого счета;
- место регистрации и фактическое место жительства;
- сведения о государственной регистрации физического лица в качестве индивидуального предпринимателя.

На этапе инвентаризации и классификации ИСПДн следует оценить необходимость и целесообразность отнесения ИСПДн к специальным системам, исходя из положений упомянутого выше совместного приказа и особенностей обработки данных в конкретной системе.

Формирование актуализированной модели угроз также является непростой и неформальной задачей. Есть мнение, что на данном этапе можно существенно снизить требования к безопасности и упростить систему защиты, признав большинство угроз неактуальными. Это не так. Актуализация угроз, безусловно, относится к полномочиям оператора, но не может выполняться произвольно. В ходе нее необходимо следовать мето-

дологии регуляторов, изложенной в нормативно-методических документах, и соблюдать установленные в них критерии оценки актуальности.

Правовые проблемы

Важная часть работы по приведению модели в соответствие с требованиями регуляторов — выявление и анализ законности оснований для обработки персональных данных и, что особенно сложно, для передачи их третьим лицам. Такими основаниями применительно к банкам являются:

- случаи, прямо предусмотренные федеральными законами;
- договор об оказании услуг физическому лицу;
- выполнение обязанностей работодателя по отношению к собственным работникам.

Договоры с физлицами должны содержать их прямое согласие на все случаи обработки данных, выходящие за пределы собственно оказания банковских услуг. Весьма сомнительными с юридической точки зрения выглядят положения договоров, предусматривающие передачу персональных данных в случаях, не предусмотренных законами, например: «Банк и Заемщик обязуются не разглашать каким-либо способом третьим лицам информацию..., включая персональные данные Заемщика, за исключением случаев, предусмотренных законодательством Российской Федерации и настоящим Договором, в том числе ... **иным лицам**, в процессе осуществления и защиты Банком своих прав, обязанностей и законных интересов, когда предоставление персональных данных происходит **в соответствии со сложившимся обычаем делового оборота**» (выделено автором). Нет в соответствующем ФЗ такого основания передачи, как обычай делового оборота.

Система безопасности ИСПДн банка

На основе исходных данных, указанных в акте классификации ИСПДн и актуализированной модели угроз, определяются механизмы безопасности, которые должны быть реализованы в системе защиты, и конкретные требования к функциональности этих механизмов.

Рассмотрим этот тезис на примере. Для абсолютного большинства ИСПДн необходимо выполнение ме-

роприятий по защите персональных данных от несанкционированного доступа (НСД) и иных неправомерных действий, включающих:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недеklarированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений.

Подсистему управления доступом рекомендуется реализовывать на базе программных средств блокирования НСД, сигнализации и регистрации (специальных, не входящих в ядро какой-либо ОС средств защиты самих ОС), электронных баз персональных данных и прикладных программ, реализующих функции диагностики, регистрации, уничтожения, сигнализации, имитации.

В свою очередь, **средства сигнализации** должны обеспечивать предупреждение операторов при их обращении к защищаемым персональным данным, а также предупреждение администратора об обнаружении фактов:

- НСД к персональным данным;
- искажения программных средств защиты;
- выхода или вывода из строя аппаратных средств защиты;
- других фактах нарушения штатного режима функционирования ИСПДн.

Такой же анализ должен быть осуществлен и при определении способов нейтрализации остальных актуальных угроз, на основании которого выбираются сертифицированные средства защиты информации с требуемой функциональностью. Имеющихся на данный момент сертифицированных средств защиты информации достаточно для реализации практически всех требований, изложенных в нормативно-методических документах ФСТЭК и ФСБ, вопреки лишь в знании их возможностей и правильном сочетании.

Сегодня созданы все необходимые условия для выполнения требований по обеспечению безопасности персональных данных, и в оставшееся до 1 января 2010 г. время все кредитно-финансовые учреждения должны построить подсистему защиты этой категории сведений ограниченного доступа. □