Уфа : УГАТУ, 2010 Вестник УГАТУ Т. 14, № 5 (40). С. 195–197

УДК 004.6

О. А. Волков

БАЗОВАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СИЛОВЫХ СТРУКТУР ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Рассмотрены основные угрозы безопасности персональных данных при использовании в информационных системах персональных данных органов государственной власти. *Информационная безопасность*; *персональные данные*

Федеральный закон № 152 от 27.07.2006 г. «О персональных данных» не только позволил решить проблему «бесхозности» информации такого типа, но и обозначил целый ряд требований к операторам информационных систем персональных данных (ИСПДн). Компьютеризация последних лет привела к переходу каталогизации на качественно новый уровень. Картотеки превратились в базы данных, открыв массу новых возможностей и создав новые проблемы. Один компьютер с успехом заменил архивные стеллажи, сетевые технологии позволили использовать удаленные обращения, в разы сократилось время на поиск и обработку информации. Новые возможности появились не только у законопослушных пользователей, у злоумышленников появилась возможность атаки ресурсов. Множество хакерских методов, методов социальной инженерии открывают злоумышленникам доступ к ИСПДн.

Необходимость защиты персональных данных (ПДн) обусловлена двумя основными факторами [1, 2]:

- конституционным правом граждан на защиту личной информации;
- широким распространением информационных систем, обрабатывающих ПДн.

Могут ли силовые структуры власти (ССВ) использовать ИСПДн в своей деятельности? Не только могут, но и должны использовать для обеспечения надлежащего уровня безопасности государственных интересов. Но если коммерческий оператор учитывает только своих клиентов, то субъектами для ССВ будут все жители региона. ИНН, паспортные данные, номера автотранспорта – все это примеры ПДн, требующих обработки в информационной системе ССВ.

Попробуем создать обобщенную модель ИСПДн, на основе базы данных, применяемой для обработки персональных данных в ССВ. Процесс создания данной модели разделим на три части:

- разработка требований к базе данных;
- проведение анализа базы данных как ИСПДн;
- разработка методики противодействия угрозам данной ИСПДн.

База данных силовых структур создается с целью обеспечения защиты безопасности государства и общества, исходя из этого, создается ее структура. Прежде всего, органы государственной власти интересует возможность учета, то есть накопление и анализ информации. Субъектами учета в данном случае будут физические лица. Физические лица сами по себе обладают рядом параметров, позволяющих их идентифицировать, отнести к определенной категории и совершать с ними ряд операций по анализу. К таким параметрам относятся, например: фамилия, имя, дата рождения и т. п. Данный тип параметров является общим для всех субъектов, его наличие в базе данных обязательно для идентификации и не может быть пропущено. Анализируя эту информацию, мы можем, к примеру, узнать, сколько мальчиков родилось в 1992 году, и спрогнозировать число «уклонистов» в 2010. Единственное, в чем мы должны быть уверены, обрабатывая данные, это в полноте предоставленной информации. Все физические лица региона, подконтрольного органу власти, должны находиться в базе; более того, информация на них должна быть в актуальном состоянии. Если год рождения не меняется в течение жизни, то фамилия может быть изменена, и не один раз. Из этого следуют два требования к формируемой базе данных. Во-первых, количество записей должно быть больше количества жителей в регионе (т. е. в среднем около двух миллионов), во-вторых, база данных должна иметь разграничение прав, как минимум, на оператора, способного вводить информацию, и на администратора, способного заниматься анализом.

Контактная информация: info@istu.ru

Кроме информации, присущей всем субъектам учета, есть информация, которая может разделять субъекты на различные группы, назовем ее дополнительной. К ней относится наличие у субъекта автотранспорта, оружия, судимостей и тому подобное.

Возможность анализа подразумевает набор определенных функций по поиску, сортировке информации в автоматическом или полуавтоматическом режиме по заданным критериям.

Создание и наполнение базы данных такого объема является задачей, рассчитанной на много месяцев, а то и лет, и подразумевает постоянную работу по внесению новых и изменению старых записей, что несет в себе жесткие требования по отказоустойчивости системы.

Основным документом при проектировании ИСПДн является приказ № 55/86/20 от 13.02.2008 г. «Об утверждении порядка проведения классификации информационных систем персональных данных». В соответствии с ним ПДн относятся ко второй категории, так как позволяют однозначно классифицировать субъект, получить о нем дополнительную информацию, но не подпадают под первую категорию. Количество одновременно обрабатываемых субъектов, как видно из требований к базе данных, более 100000. Информация, автоматически обработанная в ИСПДн силовых структур, вполне естественно может нести юридические последствия для субъекта, а значит, данная система является специальной; кроме этого, должно соблюдаться не только требование конфиденциальности, но и защита от любых несанкционированных действий. Структура системы косвенно выходит из цели ее создания: для выполнения возложенных законом функций сотрудник органов власти должен иметь доступ к данным в максимально короткие сроки из любого территориального отделения, а значит, система может быть только распределенной. Наиболее рационально создать локальную информационную систему для решения большинства административных задач, с подключением к ней пользователей по технологии удаленного доступа для просмотра информации. Система не будет иметь подключения к сетям общего пользования или международного информационного обмена, все технические средства будут находиться на территории Российской Федерации (рассмотрение сетей иного типа выходит за рамки рассмотрения данной статьи). ИСПДн ССВ изначально разрабатывается как многопользовательская, с разграничением прав доступа.

Создание специальной ИСПДн не может обойтись без построения модели угроз безопасности. Именно на основании модели и классифицируется ИСПДн. В нашей системе возможна реализация угроз безопасности, направленных на:

- уничтожение информации, содержащейся в ИСПДн;
- получение несанкционированного доступа (НСД) с целью получения, просмотра информации;
- получение НСД с целью изменения информации.

В случае уничтожения информации может иметь место как непреднамеренное (пожар, отказ оборудования и т. п.), так и преднамеренное воздействие, в остальных случаях воздействие имеет преднамеренный характер, хотя и может быть случайным в последнем случае (ошибка оператора). Наиболее опасным является целенаправленное получение НСД, так как в этом случае появляется злоумышленник, а значит, последствия будут носить противозаконный характер. Стоит отметить, что тяжесть последствий злонамеренного НСД не всегда больше непреднамеренного, например, внесение изменений в запись одного субъекта ПДн злоумышленником может быть отслежена и своевременно исправлена, в то же время отказ оборудования может поставить под угрозу существование ИСПДн в дальнейшем.

Для предотвращения уничтожения информации необходимо вести копию базы данных и поддерживать ее в актуальном состоянии. При выработке мер противодействия данной угрозе учитывается ее специфика, заключающаяся в невозможности определения точного времени, требуемого на восстановление системы, с одной стороны, и достаточно результативного механизма восстановления, с другой. Актуальная копия базы данных, чаще называемая backup и хранимая в архиве для экономии места на физическом носителе, позволит восстановить информационную систему из любого состояния. Если такой архив является кроссплатформенным, то есть может быть установлен на нескольких различных программно-аппаратных комплексах, то достигается максимальная надежность.

Для получения НСД с целью просмотра, злоумышленник может попытаться внедрить ложный объект в систему. Осуществить это в локальной, административной сети практически невозможно, так как сеть находится в охраняемом периметре и доступ к ней ограничен. Следовательно, объект будет внедрен как удаленный. Всем, в том числе и удаленным объек-

там, для получения доступа к ИСПДн необходимо пройти идентификацию. Идентификация объекта подразумевает три этапа: аутентификацию, авторизацию и аккаунтинг. Использование всех трех этапов оправданно. Каждый объект обладает своими правами в системе и может быть объединен с другими объектами в группу, тем самым упростив администрирование. Группе могут быть назначены время доступа к базе и другие параметры. Объект для подтверждения должен вводить один или несколько паролей, которые ввиду удаленности должны передаваться в зашифрованном виде, тем самым предотвращая угрозу сканирования сетевого трафика с целью завладения паролем. Данная угроза маловероятно может быть использована для непосредственного получения информации, так как, с точки зрения злоумышленника, информация носит случайный характер, а передача в зашифрованном виде не позволит ее воспроизвести. Кроме этого, для получения пароля может служить внедрение в удаленную рабочую станцию вредоносной программы, целью которой будет выявление и передача пароля злоумышленнику. Для противодействия необходимо проведение централизованной антивирусной профилактики.

Угрозы с целью получения НСД для изменения информации практически не могут быть осуществлены без поддержки изнутри. Инсайдерская активность является обязательным фактором для успешного осуществления угрозы данного типа. Именно поэтому проводится разграничение доступа не только на пользователей и администраторов, но и среди администраторов. Как видим, пользователей удобно разбить на группы, в каждой группе должен быть администратор, следящий за активностью своих пользователей и снабженный инструментарием для выявления аномалий. Администраторы должны выполнять только функции по администрированию своей части базы данных и иметь права только на это.

С целью выявления НСД в ИСПДн должен вестись лог (история действий), в логе может быть кратко отражена информация о действиях всех пользователей, системные сообщения, информация о текущем состоянии БД.

Данная модель может быть использована в качестве основной при разработке ИСПДн для любого органа государственной власти.

СПИСОК ЛИТЕРАТУРЫ

1. **Клейменов С. А.** Информационная безопасность и защита информации. Академия, 2007. 336 с.

2. **Филин С.** А. Информационная безопасность. Альфа-Пресс, 2006

ОБ АВТОРЕ

Волков Олег Алексеевич, асп. каф. защ. инф. Ижевск. гос. ун-та (ИжГТУ). Дипл. инж. по сист. и сет. (ИжГТУ, 2005). Готовит дис. в обл. защиты информации.