Защита персональных данных. Казнить нельзя помиловать?

В статье обсуждаются нормативные требования к защите персональных данных, которые должны вступить в действие уже в начале 2010 г. Рассматривается решение, обеспечивающее реализацию этих требований в соответствии с классом защиты данных.

Введение

Меры по защите персональных данных перестают быть просто нормой этики взаимодействия организации с клиентом. Участившиеся случаи "кражи личности" и мошенничества перевели их в ранг первоочередных задач, решение которых будет жестко контролироваться государством. Так, начиная с февраля 2008 г., вступило в силу сразу несколько нормативных требований, которые завершили затянувшийся период формирования основных правил взаимодействия участников рынка персональных данных. Есть четкое распределение ролей, условия и судьи – все для того, чтобы игру начали. Хотя бы ключевые игроки. Хотя бы для того, чтобы успеть максимально подготовиться к обороне и стать примером для менее крупных компаний.

Пока на подготовку к правильной расстановке акцентов "казнить нельзя, помиловать" у каждого игрока есть время, и важно его не упустить.

Прописные истины, знать которые мы обязаны

В соответствии с **Федеральным Законом от 27.07.2006 г. 152-ФЗ "О персональных данных"** любое юридическое лицо обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования и распространения. Привести информационную систему персональных данных, созданную до вступления данного Закона в силу (27.07.2006 плюс 180 дней), согласно всем требованиям, необходимо ***не позднее 1 января 2010 г.***

Законом определяются такие понятия, как "персональные данные" и "оператор персональных данных".

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе: ФИО, год, месяц, дата и место рождения, адрес, семейное положение, доходы и т.д.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Очевидно, что под определение оператора, данное государством, подпадает практически любая организация, хранящая информацию о своих сотрудниках. Следовательно, выполнять требования Закона, а в случае его нарушения – нести ответственность обязаны практически все коммерческие и государственные структуры. Так, по оценкам ФСТЭК и ФСБ, Федеральный Закон "О персональных данных" затрагивает деятельность около 7 млн юридических лиц и частных предпринимателей. Но было бы неправильным ставить в одинаковые условия компании разного по масштабу деятельности и конфигурации информационных систем уровня, требуя идентичности в мерах по защите.

Требования по обеспечению защиты персональных данных (ПДн) определяются в соответствии с классом информационной системы персональных данных (ИСПДн). Класс системы, в свою очередь, зависит от объема обрабатываемых персональных данных и модели угроз в соответствии с ***совместным приказом ФСТЭК, ФСБ и Мининформсвязи от 13.02.2008 г. "Об утверждении Порядка проведения классификации информационных систем персональных данных"***.

На основе данных о классе информационной системы персональных данных и частной модели угроз, а также ***"Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утверждена ФСТЭК 15.02.2008 г.) и "Основных мероприятиях по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" (утверждена ФСТЭК 15.02.2008 г.)*** формулируются конкретные организационно-технические требования по защите персональных данных от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы.

Довольно долго специалистами обсуждалась и перерабатывалась сама методика классификации, но последние распоряжения ФСТЭК (Федеральной службы по техническому и экспортному контролю) окончательно закрепили порядок ее проведения "Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" от 15.02. 2008, в котором описаны:

- "Базовая модель угроз безопасности ПДн при их обработке в ИСПДн";
- "Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн";
- "Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн";
- "Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн".

Контроль и надзор за выполнением перечисленных требований осуществляют:

1. Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Россвязьохранкультура);
2. Министерство связи и массовых коммуникаций Российской Федерации (Минкомсвязь РФ);
3. Федеральная служба безопасности РФ (ФСБ РФ);
4. Федеральная служба по техническому и экспортному контролю (ФСТЭК РФ).

Компаниям во главе с руководством, которые не смогли обеспечить должный уровень безопасности персональных данных, предусмотренный законодательством, грозит ***гражданская, уголовная, административная и дисциплинарная ответственность***.

За нарушения вышеприведенных нормативных актов РФ, а также ФЗ "О персональных данных" и Трудового Кодекса РФ в Кодексе об административных правонарушениях РФ и Трудовом Кодексе РФ предусмотрены следующие санкции:

1. Меры по приостановлению или прекращению обработки персональных данных, осуществляемых с нарушением требований настоящего Федерального закона.

2. Направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

3. Привлечение к административной ответственности лиц, виновных в нарушении.

4. Приостановка действия или лишение лицензий, без которых деятельность по обработке персональных данных становится незаконной.

5. Конфискация несертифицированных средств защиты информации (в т.ч. основного оборудования и программного обеспечения КИС, т.к. персональные данные обрабатываются непосредственно в КИС, а средства защиты интегрированы в стандартное оборудование и программное обеспечение КИС).

6. Административный штраф за использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации в размере:

- *на должностных лиц* – от 1 тысячи до 2 тысяч рублей;
- *на юридических лиц* – от 10 тысяч до 20 тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

7. Конфискация используемых средств шифрования.

Следуя букве закона

Несмотря на то, что законодательство РФ отводит, на первый взгляд, внушительный срок для приведения информационных систем персональных данных к соответствию всем необходимым нормам – до 1 января 2010 г., времени у операторов остается не слишком много.

Дело в том, что даже для компаний уровня SMB, не говоря уже о крупных территориально-распределенных структурах процесс создания защищенной системы персональных данных довольно сложен и предполагает комплекс действий, для реализации хотя бы части из которых обязательно придется привлекать ИТ-подрядчиков. А это уже вопрос времени и бюджета, рамки которых необходимо оценить и запланировать на 2009 год, то есть – через квартал. Именно поэтому крупные публичные компании и государственные ведомства сейчас ведут работу по защите персональных данных.

Типичный процесс создания системы защиты персональных данных предполагает последовательную реализацию этапов, но уже по составу работ можно судить о сложности и масштабах подобных проектов:

1. Обследование ИСПДн на соответствие требованиям Законодательства РФ (включая всю имеющуюся документацию и используемые средства защиты, составление перечня Пдн и определение дальнейших шагов по совершенствованию ИСПДн).
2. Классификация ИСПДн на основе собранной информации.
3. Разработка частной модели угроз ИСПДн.
4. Разработка технического задания.
5. Разработка системы защиты ПДн.
6. Макетирование и стендовые испытания.
7. Внедрение и пуско-наладка системы защиты ПДн.
8. Разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн.
9. Сертификация систем (при необходимости).

Поскольку специфика системы защиты персональных данных зависит от присвоенного ей класса, рассмотрим более подробно, как это осуществляется.

Прежде всего, напомним, что классифицируются системы по уровням защищенности в зависимости от важности накапливаемых, обрабатываемых и распределяемых ПДн. При этом определяются следующие исходные данные:

1. Категория обрабатываемых в информационной системе персональных данных – ХПД.
2. Объем обрабатываемых персональных данных (количество субъектов персональных данных, которых обрабатываются в информационной системе) – ХНПД.
3. Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе.
4. Структура информационной системы.
5. Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена.
6. Режим обработки персональных данных.
7. Режим разграничения прав доступа пользователей информационной системы.
8. Местонахождение технических средств информационной системы.

Табл. 1. Классы информационных систем

класс 1 (К1)	класс 2 (К2)	класс 3 (К3)	класс 4 (К4)
нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПДн	нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к менее значительным негативным последствиям для субъектов ПДн	нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн	нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПДн

В зависимости от объема обрабатываемых персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства устанавливаются следующие 4 класса информационных систем (табл. 1).

В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, ИСПДн присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем. Результаты классификации информационных систем оформляются соответствующим актом оператора.

Далее, с использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе "Рекомендаций по обеспечению безопасности персональных данных..." и "Основных мероприятий по организации и техническому обеспечению безопасности персональных данных...":

1. Формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа.
2. Осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

Пример защиты персональных данных

Разработанное ЕВРААС.ИТ решение по защите системы управления персоналом "Босс-Кадровик" предусматривает создание комплекса программных средств защиты всего массива данных веб-сервера "Босс-Кадровик":

- записей, хранящихся в базе данных "Босс-Кадровик";
- данных, передаваемых по сетям между веб-сервером "Босс-Кадровик" и его клиентами;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, передаваемого через сети передачи данных.

Реализация проекта позволила обеспечить:

- защиту электронного обмена данными между веб-сервером "Босс-Кадровик" и его клиентами;
- двухстороннюю аутентификацию (клиента перед веб-сервером и веб-сервера перед клиентом);

– шифрование передаваемых данных по стандартам шифрования ГОСТ 28147-89, ГОСТ Р.34.10-94, ГОСТ Р.34.10-2001, ГОСТ Р. 34.11-94;

– управление доступом клиентов к веб-серверу “Босс-Кадровик”;

– аудит действий клиентов на уровне веб-сервера и на уровне хранилища “Босс-Кадровик”;

– защиту персональных данных в хранилище “Босс-Кадровик” от просмотра и изменения привилегированными пользователями хранилища (администраторами базы данных).

Обеспечение безопасной передачи данных между веб-сервером “Босс-Кадровик” и его клиентами достигается совместным использованием веб-сервера Apache HTTP Server v.2.0.53, веб-браузера Internet Explorer 6 и комплекса современных программных средств криптографической защиты информации:

– криптопровайдера КриптоПро CSP v.3.0.x;

– программного модуля Trusted TLS;

– программного модуля Trusted Java 1.5.1.

В качестве криптопровайдера был выбран КриптоПро CSP v.3.0, так как это средство криптографической защиты информации, реализующее российские криптографические алгоритмы, разработано в соответствии с интерфейсом Microsoft – Cryptographic Service Provider (CSP). Федеральный закон “Об электронной цифровой подписи” определяет условия применения средств электронной цифровой подписи для создания систем юридически значимого электронного документооборота. Использование КриптоПро CSP в качестве средства ЭЦП в соответствии с положениями закона позволяет обеспечить равнозначность ЭЦП собственноручной подписи.

Интеграция КриптоПро CSP с операционной системой Windows позволяет использовать стандартные продукты и встраивать в разрабатываемые системы с применением различных интерфейсов Microsoft. Для всех платформ реализован протокол TLS(SSL) – модуль сетевой аутентификации КриптоПро TLS. Для всех платформ в состав КриптоПро CSP входит модуль уровня ядра операционной системы (криптопровайдер), что позволяет использовать основные криптографические функции (шифрование/дешифрование, проверка подлинности, хэширование) на уровне операционной системы.

Критические компоненты КриптоПро CSP протестированы на совместимость с ОС Windows по методикам WHQL test lab и подписаны Windows. По результатам тестов Intel Identifier Program, проведенных при участии специалистов компании Intel, версии КриптоПро CSP для платформ P4Ht и Xeon получили статус Runs great on Pentium 4 Ht и Runs great on Xeon.

Обязательным условием при выборе продукта являлось наличие необходимых сертификатов – КриптоПро CSP имеет сертификаты соответствия ФСБ.

Trusted TLS – расширенное решение Mod_SSL, реализующее российские стандарты криптографической защиты информации в веб-сервере Apache.

Trusted TLS предназначен для построения систем, использующих сертифицированные ФСБ (ФАПСИ) СКЗИ, и может быть использован в прикладной системе, где есть необходимость в создании защищенного соединения между клиентом и сервером.

Trusted Java 1.5.1 – библиотека Trusted Java реализует в Java-приложениях сертифицированные криптографические алгоритмы, предоставляемые криптопровайдером КриптоПро CSP от компании “Крипто-ПРО”. Используемые сертифицированные российские криптоалгоритмы предназначены для:

– авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями (создание и проверка ЭЦП);

– обеспечения конфиденциальности и контроля целостности информации (шифрование и имитозащита).

Библиотека поддерживает интерфейсы JCE и JSSE (защита канала передачи данных).

Для работы с провайдером JSSE, реализующим безопасные соединения в интернете, поддерживаются сертифицированные криптоалгоритмы в протоколе TLS на стороне сервера, а также двухфакторная аутентификация по ГОСТ-сертификатам на стороне клиента. Также на стороне клиента реализована поддержка прокси. Таким образом, Trusted Java позволяет использовать в полной мере провайдер JSSE для организации защищенного канала по протоколу TLS с использованием российских криптографических алгоритмов. Кроме того,

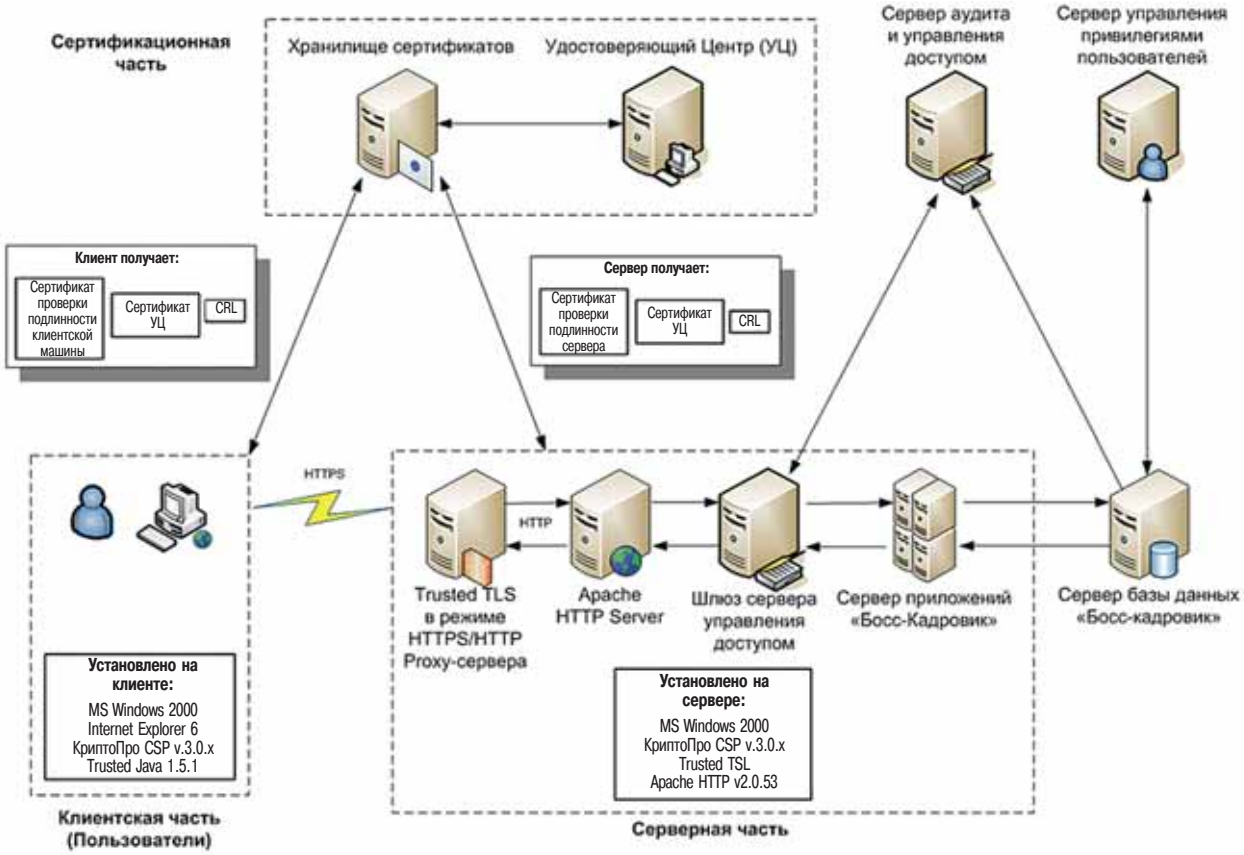


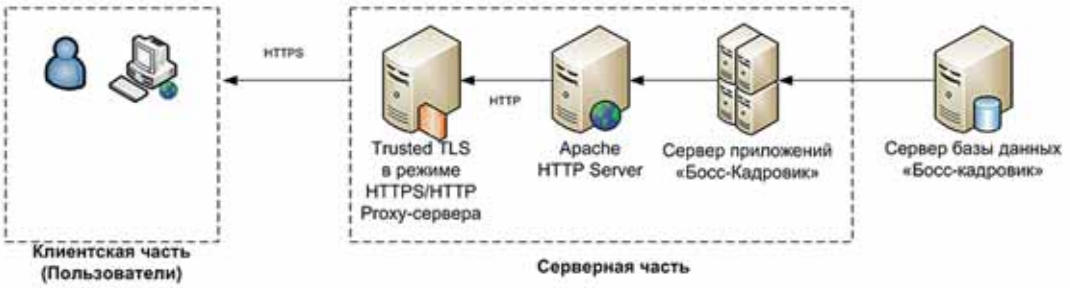
Рис. 1. Архитектура защищенного соединения веб-сервера "Босс-кадровик" и его клиентов.

компонент включает функциональность для шифрования данных, аутентификации клиента и сервера и обеспечения целостности сообщений.

Для провайдера JCE в Trusted Java реализована поддержка сертифицированных криптоалгоритмов в Службе штампов времени (TSP), предназначенной для удостоверения точного времени создания документов и их подписей.

Управление доступом клиентов к веб-серверу "Босс-Кадровик" обеспечивается реализацией соответствующих политик сервером Oracle Access Manager (OAM). Он может работать не только с веб-сервером "Босс-Кадровик", но и с широким набором LDAP-каталогов, серверов приложений, веб-серверов, серверов порталов и прикладных приложений, поставляемых ведущими производителями программного обеспечения.

Прямая цепочка передачи данных.



Обратная цепочка передачи данных.

Рис. 2. Цепочки передачи данных: "прямая" – пользовательский запрос, "обратная" – ответ от сервера..

Основные характеристики и достоинства системы:

управление доступом пользователей:

- поддержка аутентификации пользователей на основе: имен и паролей, цифровых сертификатов, смарт-карт, биометрии и др.;
- возможность взаимодействия с внешними системами с целью осуществления расширенной аутентификации и/или авторизации на основе: имен и паролей, цифровых сертификатов, смарт-карт, биометрии и др.;
- поддержка авторизации индивидуальных пользователей и авторизации групп на основе политик авторизации. Развитый аппарат для определения сложных политик доступа;
- графический интерфейс для определения защищаемых информационных ресурсов, политик доступа, а также средства тестирования определенных политик;
- авторизация к группе приложений на основе однократной аутентификации (Single Sign-On, SSO);

управление аудитом и отчетность:

- система позволяет осуществлять аудит действий клиентов, выполняемых подсистемами управления их привилегиями и контроля доступа, на основе политик аудита. Возможна запись данных аудита в базу данных, что повышает надежность и защищенность этих данных;
- система поставляется с набором предопределенных отчетов, например, по неуспешным авторизациями (по пользователям или ресурсам), по созданию, активации, деактивации пользователей, по изменению данных в учетных записях.

Реализация Oracle Access Manager использует распределенную архитектуру, которая обеспечивает высокую надежность и безопасность работы компонент, которые входят в его состав. Поддержка гетерогенной среды и мировых IT-стандартов в OAM позволяет централизованно защитить все веб-ресурсы компании. Дополнительно к средствам аудита, имеющимся в OAM, предлагается использовать мощное аудиторское решение на базе Oracle Audit Vault (OAV), которое работает непосредственно с данными из хранилища "Босс-Кадровик".

Oracle Audit Vault собирает данные аудита из баз данных таблиц контрольных журналов Oracle и MS SQL (а в ближайшем будущем – Sybase и DB2), контрольных журналов файлов операционной системы и баз данных журналов транзакций для того, чтобы собрать данные до или после существенных изменений транзакций.

OAV состоит из двух зависимых частей: Audit Vault Агента и Audit Vault Сервера. Audit Vault Сервер обеспечивает работу средств управления и контроля, работает с данными аудита, занимается построениями отчетов, отслеживанием предупреждений и управляет настройками. Audit Vault Агент на основании настроек Audit Vault сервера обеспечивает сбор информации из источников данных аудита.

Таким образом, использование Oracle Audit Vault:

- упрощает процесс отчетности по соответствию нормативным требованиям;
- контролирует выполнение политики;
- предоставляет отчеты о состоянии системы безопасности;
- помогает выявить угрозу при помощи предупреждений;
- сокращает расходы при помощи политики проведения аудита;
- предоставляет надежный и расширяемый репозиторий, тем самым обеспечивая защиту данных аудита.

На предприятии с развернутым OIM базовые данные о сотруднике автоматически считываются из хранилища "Босс-Кадровик", разбираются с учетом контекста и транслируются в целевые системы (возможно и обновление некоторых полей "Босс-Кадровик" при изменении соответствующих им полей в целевых системах). Такой подход позволяет реализовать принципы ролевого управления пользователями, которые автоматически получают необходимые им права на ресурсы в соответствии с должностными обязанностями через включение их в соответствующие группы OIM.

Логическое представление архитектуры защищенного соединения веб-сервера "Босс-кадровик" и его клиентов дано на рис. 1. Представленная на нем логическая структура для обеспечения функционирования решения на всех стадиях жизненного цикла разделена на части: клиентскую, серверную и сертификационную. Каждая часть обеспечивает выполнение собственных функциональных задач. Задачи частей не пересекаются. Архитектура описанного решения определяет две цепочки передачи данных (рис. 2):

– прямая (пользовательский запрос);

– обратная (ответ от сервера).

Итак, осталось чуть больше года, пора подумать о запятой, которую могут поставить – и не в том месте.

Елена Гущина,
компания "ЕВРААС.ИТ"