Проблемы информационной безопасности и защиты персональных данных на предприятиях ТЭК

Еще недавно считалось, что применение ИТ на предприятий ТЭК связано в первую очередь с управляющей деятельностью и работой офисных подразделений, то есть ИТ – это та сфера, которая не оказывает решающего влияния на течение основного бизнеса. А значит, вопросы информационной безопасности, играющие существенную роль для организаций, например, финансового сектора, здесь не так сложны и решаются значительно проще, по стандартной схеме: на периметре – межсетевой экран, на рабочей станции – антивирус. Широкое развитие автоматизации, совершенствование систем АСУ ТП, внедрение ERP и систем электронного документооборота привело к значительному увеличению роли ИТ-технологий в организации стабильной и успешной работы предприятий ТЭК, что не могло не сказаться на появлении новых рисков информационной безопасности, которые, как ни прискорбно, по сложившейся традиции редко кто брал в расчет при построении и модернизации этих систем.

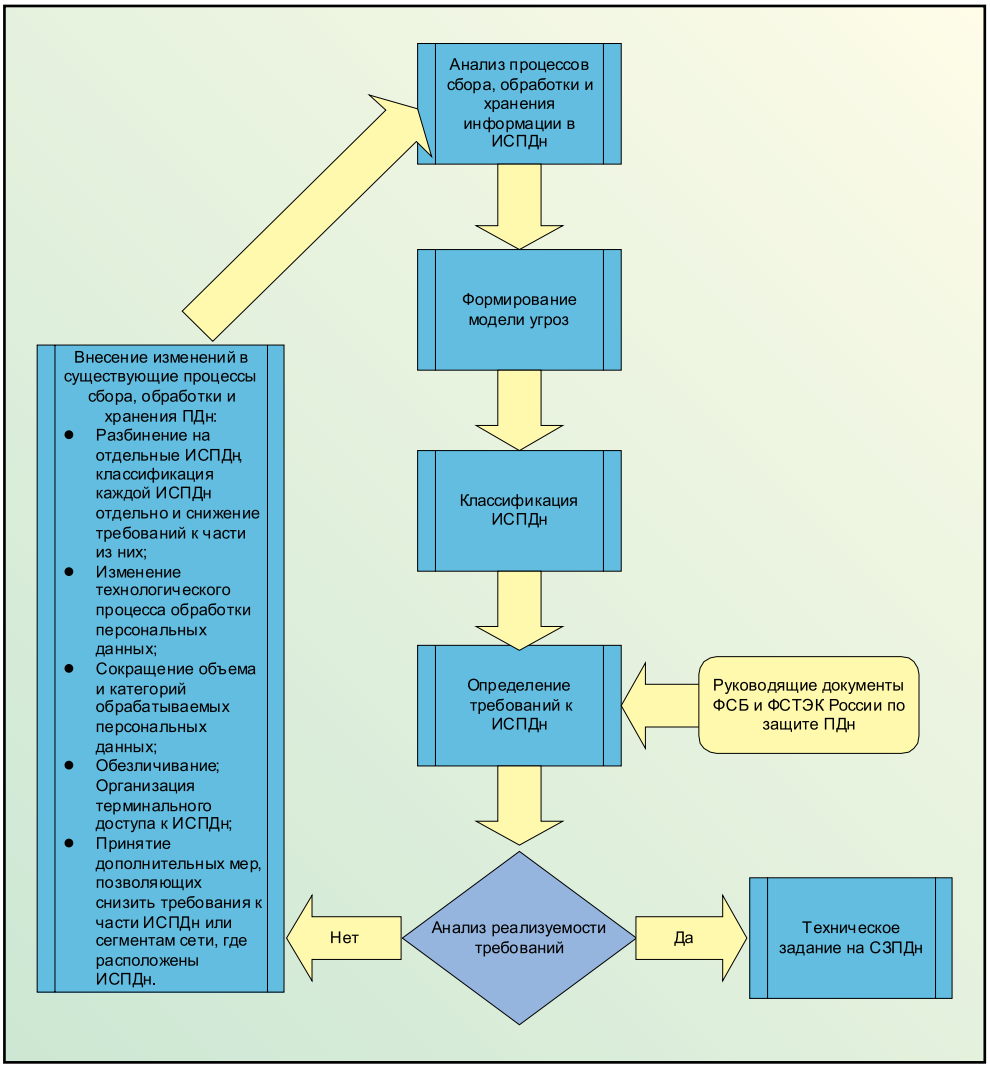
Многие холдинги нефтегазовой отрасли образовались путем многократных слияний и поглощений различных компаний со своей сложившейся ИТ-инфраструктурой и культурой информационной безопасности. Поэтому единой политики информационной защиты в этих структурах, как правило, не существует. Управляющие компании зачастую не в курсе, какими средствами обеспечивается защита информации на местах в конкретном подразделении, какие организационные процедуры и документы в них действуют. Сведения об используемых средствах защиты и их настройках можно почерпнуть только у сетевых и системных администраторов, обладающих неограниченным доступом ко всей информации. Нет ни единой политики информационной безопасности (или она действует исключительно на бумаге), ни четких инструкций для пользователей и администраторов.

А между тем, ценность обработанной и структурированной информации, циркулирующей в системах электронного документооборота, ERP или системах расчетов с клиентами холдинга, стала несоизмеримо выше, чем раньше, а значит, значительно повысились риски и размеры потенциального ущерба, в том числе и от простоя систем, который может исчисляться в миллионах долларов.

В этих условиях затраты на информационную безопасность уже не кажутся запредельными – стоимость решения инцидентов значительно выше, и подход с надеждой на русский "авось" уже не проходит. Но и принцип "бездумного латания дыр", доставшихся в наследство от периода бурного развития технологий и систем, тоже нельзя назвать приемлемым, поскольку степень защищенности системы определяется степенью защищенности ее самого слабого звена. Таким образом, без целостной концепции построения системы защиты как комплекса связанных правовых, технических и организационных мер создание эффективной системы невозможно. Действенным подходом к построению целостной многоуровневой системы информационной безопасности может стать разработка единого внутрикорпоративного стандарта или политики информационной безопасности, действие которой распространяется на все предприятия, входящие в холдинг, с учетом специфики каждого из них. При этом апробированные типовые технические решения и организационные процедуры унифицированно распространяются на все организации холдинга, осуществляется централизованный мониторинг и разбор инцидентов информационной безопасности, а в случае нехватки квалифицированного персонала на местах управление средствами защиты и настройки безопасности телекоммуникационной инфраструктуры осуществляются из центра.

Защита персональных данных является одной из составляющих общей проблемы обеспечения информационной безопасности на предприятиях ТЭК. Как и в любой современной организации, на предприятии ТЭК используются системы электронного документооборота, электронные справочники, автоматизированные системы кадрового и бухгалтерского учета, биллинга, электронной почты и т.п., содержащие персональные данные, которые необходимо защищать в соответствии с недавно принятым законом о персональных данных. Само принятие закона и нормативные документы, выпущенные ФСТЭК и ФСБ России в этой связи, дали толчок активным действиям в области информационной безопасности операторов персональных данных, к которым можно отнести практически любую организацию на территории Российской Федерации.

При этом общая ситуация с обеспечением информационной



безопасности на предприятиях ТЭК и уровень осведомленности персонала, в том числе и лиц, отвечающих за соблюдение режима информационной безопасности, особенно в регионах, оставляет желать лучшего.

С какими же наиболее вероятными проблемами столкнется предприятие ТЭК как оператор персональных данных?

В настоящее время активно проявляется тенденция к выделению отдельных подразделений крупных холдингов и корпораций, не занятых в профильной деятельности, в отдельные юридические лица, например эксплуатирующие подразделения, которые в том числе отвечают за работу информационных систем персональных данных (ИСПДн) по всему холдингу и связанной телекоммуникационной инфраструктуры. Таким образом, "размывается" понятие оператора персональных данных, поскольку информация, обрабатываемая в такой ИСПДн, принадлежит одному юридическому лицу, а средства ее обработки (СВТ, телекоммуникационное оборудование, линии связи) – другому.

Не проще ситуация и в случае холдинга, состоящего из нескольких юридических лиц, связанных единой управляющей компанией, эксплуатирующей, например, единую централизованную биллинговую систему, в которой обрабатываются данные более ста тысяч физических лиц, являющихся к тому же абонентами различных организаций холдинга. В этом случае обработку персональных данных управляющей компанией уже нельзя считать осуществляемой в рамках договора с физическим лицом на абонентское обслуживание, поскольку он заключен с другим юридических лицом. Управляющей организации необходимо будет оформить согласие физического лица на автоматизированную обработку его персональных данных и уведомить соответствующий уполномоченный орган по защите прав субъектов персональных данных об осуществлении обработки таких персональных данных.

Кроме упомянутых выше и других юридических вопросов, которые неизбежно придется решать при построении систем защиты персональных данных, необходимо отметить и жесткие требования регуляторов по технической защите персональных данных.

Централизация всех ресурсов в руках управляющей компании, конечно, значительно повышает эффективность обработки и хранения данных в рамках холдинга, но и существенно повышает риски информационной безопасности в отношении этих данных, что и выражается в присвоении таким ИСПДн первого или второго класса при классификации в соответствии с "Порядком проведения классификации информационных систем персональных данных" (совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20). Немногие организации готовы сейчас к выполнению всех требований для ИСПДн 1 и 2 класса в соответствии с нормативным документом ФСТЭК России "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" не только финансово, но и организационно: речь идет об обязательных мероприятиях по защите персональных данных от утечки за счет ПЭМИН, аттестации ИСПДн, а также о получении лицензии на осуществление деятельности по технической защите конфиденциальной информации для организации-оператора.

Можно предложить несколько вариантов снижения затрат на создание систем защиты персональных данных для таких систем:

- максимальное использование уже имеющихся сертифицированных средств защиты и/или возможностей ОС и прикладного ПО, сертифицированных или имеющих перспективы сертификации в системах сертификации ФСТЭК России или ФСБ России;
- разделение информационной системы сертифицированными межсетевыми экранами на отдельные ИСПДн, классификация каждой ИСПДн отдельно и снижение требований к части из них;
- изменение технологического процесса обработки персональных данных путем:
  - сокращения персонала (и числа АРМ), участвующих в обработке персональных данных;
  - выделения нескольких систем персональных данных, например путем разделения функций и недопущения одновременной обработки данных из разных систем;
  - обезличивания части ИСПДн путем перехода на абонентские номера, номера лицевых счетов и т.п.;
  - организации терминального доступа к ИСПДн;
  - исключения части персональных данных (например данных о здоровье и/или других персональных данных первой категории) путем хранения на бумажных или других носителях вне ИСПДн;
- принятие дополнительных мер, позволяющих снизить требования к части ИСПДн или сегментам сети, где расположены ИСПДн.

Что из этого является приемлемым в той или иной ситуации, зависит от множества факторов, в первую очередь от специфики информационных систем и имеющегося технологического процесса обработки и хранения персональных данных, наличия на предприятии ТЭК грамотных специалистов, квалификации подрядной организации и т.п.

Выбор сертифицированных средств защиты информации для организации системы защиты персональных данных тоже имеет свои нюансы.

Несмотря на содержащиеся в нормативном документе ФСТЭК России "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" положения о том, что для обеспечения безопасного межсетевого взаимодействия в ИСПДн 2 класса рекомендуется использовать МЭ не ниже четвертого уровня защищенности, а в ИСПДн 1 класса – не ниже третьего, список требований к подсистеме межсетевого экранирования в ИСПДн 1 и 2 класса в соответствии с "Основными мероприятиями по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" гораздо шире, чем требования к межсетевым экранам 3 и 4 класса защищенности в соответствии с РД "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа". В первую очередь это касается функций возможности сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети, возможности трансляции сетевых адресов, динамического контроля целостности программной и информационной части межсетевых экранов, дистанционной сигнализации попыток нарушения правил фильтрации, регистрации и учета запросов прикладного уровня, программируемой реакции на события в МЭ, оперативного восстановления свойств экранирования после сбоев и отказов. Многие из этих функций не поддерживаются некоторыми межсетевыми экранами, как российского производства, так и популярных западных производителей, сертифицированными по 3 классу.

Таким образом, при выборе сертифицированных средств защиты лучше все же предпочесть те, в сертификате которых явно сказано о возможности применения данного средства в ИСПДн соответствующего класса.

Если рассматривать организационный аспект проблемы обеспечения защиты персональных данных, то различными нормативными документами ФСТЭК, ФСБ России, распоряжениями уполномоченного органа (в настоящее время Федеральная служба по надзору в сфере связи и массовых коммуникаций (Россвязькомнадзор)) установлено более двух десятков организационно-распорядительных документов, которые должны быть разработаны на предприятии и которые призваны регламентировать все вопросы, связанные с обработкой и хранением персональных данных, что налагает на и без того малочисленные службы информационной безопасности предприятий ТЭК дополнительную и немалую нагрузку.

Что же остается делать? Проблем и вопросов много, решения не лежат на поверхности, кроме того, на оператора законом возложена вся ответственность как за урегулирование правовых вопросов обработки персональных данных, так и за внедрение технических и организационных мер по защите персональных данных. Ответ – поскорее начать работу. Конечно, внедрение комплексной системы защиты персональных данных в полном соответствии с требованиями нормативных документов регуляторов в срок до 1 января 2010 года – неосуществимая мечта, но "дорогу осилит идущий"... Грамотно спланированная работа внутри организации, привлечение внешних квалифицированных специалистов в области информационной безопасности позволят адекватно оценить имеющиеся угрозы персональных данных, спроектировать и внедрить единую экономически эффективную комплексную систему защиты, как отвечающую требованиям регуляторов, так и реализующую надежную степень защищенности критичных информационных ресурсов предприятия.

Екатерина Яблокова,
заместитель директора
по развитию бизнеса,
компания Stonesoft