



Как защитить персональные данные

Подборка статей LETA IT-company



LETA IT-company | LETA IT-company (www.leta.ru) – первый российский оператор типизированных ИТ-услуг, обеспечивающий заказчикам комплексные решения в области информационной безопасности. Спектр услуг LETA IT-company включает все этапы жизненного цикла построения информационной безопасности на предприятии – аудит, консалтинг, внедрение, сопровождение.

Содержание

cnews

**БАНКОВСКИЕ
ТЕХНОЛОГИИ**

**Персональные
данные**

Information Security
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

iBUSINESS

Manager
АССОЦИАЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Manager
АССОЦИАЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Защита персональных данных: откладывать больше нельзя.....	4
Вениамин Левцов, директор департамента развития Илья Новиков, руководитель направления информационной безопасности	
Персональные данные. Будни банковской безопасности.....	10
Евгений Царев, заместитель директора департамента развития	
Меры и средства защиты персональных данных.....	12
Вениамин Левцов, директор департамента развития Николай Зенин, руководитель направления защиты коммерческих тайн	
Фактическая защищенность персональных данных на предприятиях с различной формой собственности.....	17
Олег Губка, руководитель отдела поддержки и сопровождения продаж	
Надо ли регистрироваться. Кто сказал, что надо уведомлять Роскомнадзор.....	19
Илья Новиков, руководитель направления информационной безопасности	
Защита персональных данных: антикризисный подход.....	23
Николай Конопкин, заместитель директора департамента внедрения и консалтинга	
Как превратить предприятие в легитимного оператора персональных данных.....	26
Николай Конопкин, заместитель директора департамента внедрения и консалтинга	
О LETA IT-company.....	31



Вениамин Левцов,
директор департамента
развития



Илья Новиков,
руководитель направления
информационной
безопасности

cnews

CNews
май, 2009

Защита персональных данных: откладывать больше нельзя

Закон "О персональных данных" (№152-ФЗ) поставил перед большинством российских компаний сложнейшую задачу, которую предстоит решить уже в этом году. Серьезность государства в этом вопросе очевидна: сформирована нормативная база, определена ответственность, контролирующие органы получили соответствующие полномочия, растет количество проверок. Между тем, сегодня далеко не все компании, обрабатывающие персональные данные, осознают необходимость их защиты и до конца понимают реальность и масштаб рисков невыполнения закона.

С каждым месяцем вопрос защиты персональных данных (ПДн) становится острее. У организаций, обрабатывающих такую информацию, остается все меньше времени до 1 января 2010 года, чтобы привести свои информационные системы в соответствие с федеральным законом №152-ФЗ. То и дело от Роскомнадзора поступают недвусмысленные сигналы о необходимости подачи заявки на регистрацию в качестве оператора ПДн. Если компания этого не сделала, она нарушает установленные законом требования, и ее деятельность может быть приостановлена регулирующим органом. И, судя по действиям Роскомнадзора, массовые проверки уже не за горами.

Закон №152-ФЗ несет в себе еще одну угрозу – дает дополнительный инструмент недобросовестным конкурентам. Что мешает подать заявление от лица субъекта персональных

данных (конкретного гражданина) о нарушении его прав компанией, которой он сообщил личную информацию? Предприятие ждет еще одна проверка, отвлекающая силы от основного бизнеса. Поэтому задача построения защиты персональных данных выходит далеко за рамки полномочий департамента информационной безопасности. Ведь невыполнение требований закона несет угрозу не просто информационным ресурсам или интересам отдельных клиентов – возникает угроза для нормального функционирования самого бизнеса. Именно поэтому задача построения защиты персональных данных выходит далеко за рамки полномочий департамента информационной безопасности, и все важнейшие решения по проекту "Построение защиты персональных данных" должны приниматься на уровне высшего менеджмента организации.

"Подавляющее большинство организаций до сих пор не запустило проекты по приведению информационных систем в соответствие с положениями закона "О персональных данных", – отмечает исполнительный директор LETA IT-company Андрей Конусов. – Промедление было связано, прежде всего, с тем, что лишь совсем недавно появился полный массив нормативных актов регуляторов. Вторая причина в том, что организациям очень непросто решиться на серьезные траты и реорганизацию ряда бизнес-процессов, сохраняя традиционную надежду на то, что "беда пройдет стороной". Но, как показывает практика, государство не изменило своих намерений добиться реализации положений закона "О персональных данных" – это наглядно демонстрируют массовые проверки, которые уже начали проводить территориальные подразделения Роскомнадзора. В этой ситуации можно обратиться к специализированным ИБ-компаниям, предлагающим услуги по построению информационных систем ПДн. Но следует помнить, что и их ресурс ограничен. Предпринимать конкретные шаги в соответствии с требованиями 152-ФЗ необходимо как можно скорее, не дожидаясь, когда в дверь постучит проверка".

Типичные заблуждения операторов ПДн

Несмотря на то, что вопросы защиты персональных данных в России достаточно молоды, уже начали складываться определенные заблуждения в данной области. Приведем основные из них.

Первое – это уверенность, что пока можно ничего не делать и подождать, пока кого-то накажут. Такая компания не несет пока никаких затрат, не обучает сотрудников и не задумывается об изменении сложившихся процессов обработки ПДн. И надеется, что первые же громкие случаи процессов или каких-то санкций заставят регулирующие органы внести существенные коррективы. Например, значительно расширить список средств, разрешенных для использования в системах защиты ПДн, или сдвинуть сроки готовности системы защиты ПДн. Но такая компания, тем не менее, сильно рискует. Санкции, предусмотренные существующим законодательством, существенны. Сценарии, которые могут привести к наложению санкций, вполне реалистичны. Быстро выполнить все работы – от получения лицензии ФСБ до изменения отдельных

процессов обработки данных – в ходе проверки попросту невозможно.

Другое заблуждение – убежденность в том, что действие закона не распространится именно на "нашу" компанию. Соответственно, тоже можно ничего не делать. Сторонники такого подхода приводят разные аргументы. Например, что в компании не ведется автоматизированная обработка персональных данных, и все делается на бумаге. Другие компании говорят: "У нас большая компания с иностранным капиталом, базы данных физически находятся на зарубежных площадках. Да и вообще – кто нас тронет?". Встречается и надежда на "блестящих юристов", которые докажут, что компания не является оператором ПДн. А некоторые считают, что если не подать заявку на оператора ПДн, то и с проверкой никто и не придет.

Однако в большинстве случаев регулирующие органы не разделяют подобную позицию, и если компания попадет в поле надзора, санкции окажутся неминуемы. "Лазейки" в действующей нормативной базе пока не выявлены, а если они и найдутся, то они будут немедленно закрыты.

В чем заключаются требования закона?

Закон №152-ФЗ призван защитить права и свободы человека при обработке его личной информации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну. Персональные данные – это любая информация, относящаяся к определенному лицу: ФИО, адрес, номер телефона, семейное, социальное, имущественное положение, образование, профессия, размер доходов, отношение к религии, данные о здоровье, хобби – перечень поистине нескончаем. Также в законе определено понятие "оператор персональных данных" – это организация, которой свои персональные данные доверил сам человек, или другая организация, обрабатывающая их.

По сути, закон ставит своей целью ввести достаточно жесткие ограничения, которым должен следовать оператор персональных данных. Как уже упоминалось, он устанавливает дату, к которой информационные системы ПДн, созданные до вступления закона в силу, должны быть приведены в соответствие с его требованиями – не позднее 1 января 2010 года. Кроме того, оператор персональных данных в большинстве случаев обязан направить в уполномоченный государственный орган соответствующее уведомление.

Регуляторы и персональные данные

В соответствии с №152-ФЗ, в орбиту процессов, связанных с защитой ПДн, вовлечены три органа государственной власти: ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций. Область ответственности у каждого из них своя. ФСБ традиционно курирует вопросы защиты информации с использованием средств шифрования (криптографии). ФСТЭК России осуществляет контроль защиты информации с применением технических средств. Одна из его компетенций – подтверждение отсутствия в средствах защиты информации недекларируемых ("шпионских") возможностей. Роскомнадзор

является основным исполнительным и надзорным органом по защите прав физических лиц, чьи персональные данные обрабатываются.

Роскомнадзор обладает следующими правами: проводить проверку сведений, содержащихся в уведомлении, поданном оператором; привлекать для такой проверки другие государственные органы (ФСБ, ФСТЭК); принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований закона; обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн и представлять их интересы в суде. А также направлять заявления в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия его лицензии; направлять в правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел в связи с нарушением прав субъектов ПДн; привлекать к административной ответственности лиц, виновных в нарушении закона.

Список полномочий весьма внушительный – очевидно, что у Роскомнадзора достаточно рычагов воздействия практически на любую организацию. На практике регулировать данную сферу деятельности должен именно Роскомнадзор, а ФСБ и ФСТЭК будут привлекаться для контроля за реализованными мерами защиты ПДн. Дело в том, что организации, эксплуатирующие информационные системы ПДн определенных классов, должны получить лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации. Кроме того, технические средства, которые будут использованы для защиты ПДн, необходимо сертифицировать в ФСТЭК. Именно методики ФСТЭК должны быть положены в основу "Модели угроз" для каждой информационной системы, обрабатывающей ПДн. Этот документ предстоит разработать каждому оператору. На выполнении этих аспектов, скорее всего, и будут сфокусированы сотрудники ФСТЭК, привлекаемые для проверок.

Закон также требует, чтобы организации, эксплуатирующие информационные системы ПДн определенных классов и передающие ПДн через общедоступные и международные сети, обеспечили их защиту с использованием криптографических средств. А деятельность по внедрению шифровальных (криптографических) средств, как и по разработке телекоммуникационных систем, защищенных с использованием данных средств, подлежит лицензированию в органах ФСБ. Так что специалисты ФСБ в первую очередь уделяют внимание наличию необходимых лицензий и использованию средств криптографической защиты, перечисленных в реестре ФСБ.

Что такое "категория персональных данных"

Законодательство вводит новое понятие – "категория персональных данных", всего таких категорий – четыре. К четвертой, наиболее простой, относятся обезличенные и (или) общедоступные персональные данные. В третью включается информация, позволяющая идентифицировать субъекта ПДн. Во вторую категорию входят данные, позволяющие не только идентифицировать субъекта, но и получить о нем дополнительную информацию. И, наконец, самая высокая,

требующая наиболее серьезной защиты, первая категория объединяет данные, в которых отражены расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь. В соответствии с достаточно понятными критериями, каждый вид ПДн относится к определенной категории, а каждая система, обрабатывающая ПДн, должна быть отнесена к конкретному классу. На класс влияет категория данных и другие признаки (распределенность информационной системы, количество записей ПДн в ней и т.д.). Очевидно, что уровень защищенности ИС должен соответствовать критичности данных. Именно поэтому для различных классов вводятся разные требования по степени защиты. Итак, чем менее детальную информацию можно получить о субъекте ПДн, чем меньше записей в системе и чем менее она распределена – тем ниже требования к защитным механизмам. С практической точки зрения крайне важно представить систему ПДн как относящуюся к "низшему" классу. Это позволит минимизировать затраты на обеспечение защиты персональных данных.

Ответственность за нарушение закона

Ответственность при невыполнении требований закона, увы, достаточно серьезна, чтобы, по крайней мере, принять ее к сведению. Проанализировав КоАП РФ и УК РФ, можно выделить ряд статей, в соответствии с которыми будет определяться ответственность за нарушение требований по защите ПДн. КоАП Статья 5.39 – отказ в предоставлении гражданину информации. Ответственность – штраф до 1 000 руб., но также это может явиться основанием для ответственности по статье 3.12 (Административное приостановление деятельности). КоАП Статья 13.11 – нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах. Ответственность – штраф до 1 000 руб.

КоАП Статья 13.12 – нарушение правил защиты данных. Ответственность – штраф от 10 000 до 20 000 руб. с конфискацией не сертифицированных средств защиты информации или административное приостановление деятельности на срок до 90 суток. УК Статья 137 – нарушение неприкосновенности частной жизни. Ответственность может достигать до штрафа в размере ЗП осужденного за 18 месяцев или ареста на 6 месяцев. УК Статья 140 – отказ в предоставлении гражданину информации. Ответственность – штраф до ЗП за 18 месяцев либо лишение права занимать ряд должностей или заниматься определенной деятельностью. УК Статья 171 – незаконное предпринимательство. Ответственность – до 5 лет лишения свободы со штрафом в размере ЗП осужденного за 6 месяцев.

Подчас приходится слышать, что пока эти статьи не работают и реального преследования никто осуществлять не собирается. Увы, это не совсем так – правоприменительная надзорная практика уже начинает складываться. Давайте представим несколько типичных ситуаций.

Пример №1. Компания получает письмо от гражданина, данные которого ранее получила и включила в свои базы, с просьбой предоставить ему информацию о том, как ведется обработка его ПДн. Что им движет – непонятно. Возможно, искренний интерес, возможно, природная любовь к конфликтам, а может и недобрый умысел. В любом случае он имеет право на такое обращение в соответствии со статьей 14, частью 4 закона №152-ФЗ. Но компания не готова к тому, чтобы дать исчерпывающий ответ в отведенное время. Она не предоставляет затребованную информацию или предоставляет ее не полностью. Клиент, не получив в указанные в законе сроки ответ, обращается с жалобой в Роскомнадзор. Тот направляет в органы прокуратуры запрос о возбуждении уголовного дела в связи с нарушением прав субъекта персональных данных. Возможная ответственность: по КоАП ст.5.39 или по УК ст.140. И вот у вас под дверью прокурорская проверка.

Пример №2. Компания поспешно регистрируется в качестве оператора персональных данных. При этом многие аспекты опускаются или оставляются на будущее. В определенный момент компания получает предписание из Роскомнадзора о проверке информации, указанной в заявке на регистрацию в качестве оператора. При документальном изучении дополнительных данных Роскомнадзор делает предварительный вывод о недостаточности мер по защите ПДн. Например, сотрудникам Роскомнадзора не предъявляются копии сертификатов на средства защиты информации, не демонстрируются лицензии ФСТЭК, ФСБ или документы, описывающие модель угроз и поведение потенциального нарушителя. После чего Роскомнадзор направляет обращение в ФСТЭК и/или ФСБ по вопросу проведения внеплановой проверки организации с целью выяснения степени выполнения требований по обеспечению защиты ПДн.

В ходе проверки выявляется, что данная организация эксплуатирует информационную систему определенного класса и в связи с этим должна была получить лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК. Лицензии данная организация не имеет, и работ по ее получению она не начинала. ФСТЭК направляет отчет о проверке в Роскомнадзор, который, в свою очередь, направляет в органы прокуратуры или другие правоохранительные органы материалы для решения вопроса о возбуждении дела. Возможная ответственность: по КоАП ст.13.12 или по УК ст.171.

Необходимо отметить и тот факт, что в УК РФ уже внесены изменения (статья 137), ужесточающие ответственность за нарушения, затрагивающие неприкосновенность частной жизни. Они вступят в силу с 1 января 2010 года.

Чем регламентирована защита ПДн

Все законодательные и нормативные акты по защите ПДн можно разбить на две группы: общедоступные и закрытые. Перечень общедоступных правовых актов известен, но и к закрытым документам доступ получить несложно. По сути, это методические рекомендации, которым оператор ПДн должен следовать. Выпустил эти руководящие документы ФСТЭК, они носят гриф "Для служебного пользования", но

предоставляются всем заявителям. Так что для их получения достаточно письменно обратиться в подразделение ФСТЭК по месту нахождения организации. Документы следующие: "Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн (информационной системе персональных данных)"; "Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн"; "Базовая модель угроз безопасности ПДн при их обработке в ИСПДн"; "Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн". К открытым специальным актам по данной теме относятся также руководящие документы ФСБ, которые можно найти по ссылке <http://www.rsoc.ru/main/directions/874/916.shtml>. Там же опубликован ряд открытых актов по ПДн, а также документы Роскомнадзора, регулирующие порядок регистрации оператора персональных данных.

Даже если построением системы занимается сторонняя компания, запрос на получение документов направить нужно. Причина проста – в случае проверки предприятие будет гораздо лучше выглядеть в глазах сотрудников ФСТЭК или ФСБ, если они увидят номерные копии руководящих документов среди прочей документации по проекту построения защиты ПДн. Если даже проверка выявит какие-то огрехи, будет учтено, что вы честно пытались разобраться, привлекали людей, изучали руководящие документы, закупили сертифицированные средства защиты. Все это, безусловно, смягчит возможные последствия.

Требования к средствам защиты ПДн

Закон предполагает, что оператор применяет специализированное программное и аппаратное обеспечение в процессах сбора, обработки, передачи и хранения ПДн. Как уже упоминалось, средства защиты ПДн должны обладать сертификатами ФСТЭК или ФСБ. К счастью, регулярно обновляемые реестры всех этих средств доступны на официальных сайтах ФСТЭК и ФСБ.

- Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00: http://www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls.
- Перечень средств защиты информации, не содержащей сведений, составляющих государственную тайну: <http://www.fsb.ru/fsb/supplement/contact/lasz/perechen.htm>.

В списках преобладают продукты отечественных производителей, но в последнее время все больше западных решений успешно проходят действующие системы сертификации. Так что с каждым годом выбор средств все более расширяется. Вполне реальна ситуация, когда в реестре упоминается средство, аналогичное тому, что уже установлено в компании, но не прошло процедуры сертификации. Если так, то это средство не будет рассматриваться проверяющим как надлежащий механизм защиты ПДн. Выходов в такой ситуации два: или переходить на использование сертифицированных средств или подавать на сертификацию уже применяемые. К сожалению, сертификация – очень непростая процедура, требующая вовлечения специализированной аккредитованной тестовой лаборатории, подготовки объемной документации о возможностях системы, предоставления исходных кодов. Кроме того, это может потребовать ощутимых расходов и займет не менее 6 месяцев.

В соответствии с руководящими документами регуляторов для некоторых классов ИСПДн необходимо внедрить систему защиты, которая может состоять из 10 подсистем. Среди них: подсистемы антивирусной защиты; защиты от НСД; анализа защищенности и выявления уязвимостей; криптографической защиты информации; маршрутизации, коммутации и межсетевое экранирование; обнаружения вторжений. В ряде случаев (если это прямо указано в разработанной модели угроз или информационной система ПДн относится к первому классу) предполагается также внедрение и специфических систем, называемых "подсистемами защиты информации от утечки по техническим каналам". Они защищают персональные данные: от утечек по цепям электропитания и заземления; от утечек за счет побочных электромагнитных излучений и наводок; от утечек по акустическому (виброакустическому) каналу; от утечек за счет акустоэлектрических преобразований и высокочастотного наводнения.

В таблице "Перечень подсистем ИБ в зависимости от класса ИСПДн" перечислены классы информационных систем ПДн и показано, какие подсистемы информационной безопасности должны быть внедрены для каждого класса, согласно руководящим документам ФСТЭК.

Перечень подсистем ИБ в зависимости от класса ИСПДн

	Антивирусная защита	Защита от НСД	Анализ защищенности и выявление уязвимостей	Подсистема обнаружения вторжения	Подсистема маршрутизации, коммутации и межсетевого экранирования	Подсистема криптографической защиты информации
ИСПДн 1 (распред.)	+	+	+	+	+	+
ИСПДн 1 (локальн.)	+	+	+	-	-	+
ИСПДн 2 (распред.)	+	+	+	+	+	-
ИСПДн 2 (локальн.)	+	+	+	-	-	-
ИСПДн 3 (распред.)	+	+	+	+	+	-
ИСПДн 3 (локальн.)	+	+	+	-	-	-

Источник: LETA IT-company, 2009

Подсистема криптографической защиты информации необходима только для ИСПДн, удовлетворяющих определенным условиям. В частности, ИСПДн должна быть многопользовательская с равными правами доступа к информации.

В связи с этим можно дать практический совет. Следует рассмотреть возможность максимально полного использования сертифицированных средств защиты. Если же удастся снизить класс системы ПДн, то требования будут значительно скромнее. При этом начать надо с возможного сужения сегмента сети организации, в которой ведется обработка ПДн. Снизил класс системы ПДн, ограничили область обращения ПДн, выбрали оптимальный состав сертифицированных средств для защиты только данной области – и затраты станут значительно ниже.

Встречаются, правда, сложные случаи, когда ПДн используются в рамках многофункциональных информационных систем уровня всей организации, например, банковских АБС. Такие системы, очевидно, не имеют сертификатов ФСТЭК, но даже получение их для одной версии не решит проблемы. Ведь эти ИС постоянно модернизируются – поддержание актуальности сертификатов на них в существующей системе сертификации невозможно. Пожалуй, единственное, что можно посоветовать в таком случае, – это обратиться в регулирующий орган с описанием проблемы. Хочется верить, что требования регуляторов после некоторого периода применения претерпят ряд изменений, которые будут предусматривать какой-то выход из данной ситуации.

Приглашать консультанта или делать самим?

Как это часто бывает, перед руководством встает классическая дилемма: использовать ресурсы собственных сотрудников или привлечь профессиональную компанию-консультанта. Для ее решения можно посоветовать ответить на несколько вопросов. Достаточно ли у сотрудников организации квалификации, чтоб выполнить требования закона № 152-ФЗ? Есть ли у них

понимание того, сколько времени займет и каких ресурсов потребует решение задачи по обеспечению соответствия закону №152-ФЗ? Кто из руководителей департаментов готов взять на себя ответственность за эффективный ход проекта по построению системы защиты ПДн? Какие действия должны быть предприняты для подачи уведомления от оператора ПДн? Как выполнить требования по защите ПДн, определенные в руководящих документах регулирующих органов, и не нарушить бизнес-процессы организации? Как минимизировать затраты на решение задач по обеспечению соответствия закону?

Возможно, в компании есть специалисты, которые служили ранее в подразделениях ФСБ или ФСТЭК и знакомы с подходом регуляторов к вопросу защиты конфиденциальной информации. Они знают основные руководящие документы, в которых эти требования определены, им известно, как подаются заявки на лицензии ФСБ и ФСТЭК. Вовлечение таких специалистов, безусловно, окажет огромное содействие ходу проекта. Но надо отдавать себе отчет, что построение системы защиты ПДн – многоплановый проект, он затрагивает различные аспекты деятельности компании. Скорее всего, упомянутый выше специалист будет готов участвовать в нем только как эксперт, но не как руководитель.

Наиболее эффективен подход, при котором для исполнения работ по проекту привлекается внешняя компания – интегратор информационной безопасности, но при этом организуется рабочая группа внутри предприятия. Правда, он, конечно, потребует дополнительных затрат на услуги подрядчика. В рабочую группу включаются следующие сотрудники компании: руководитель высшего звена в качестве спонсора проекта, глава департамента информационной безопасности как руководитель проекта и главный ответственный за его ход, глава или ведущий сотрудник ИТ-департамента, специалисты, имевшие опыт службы в ФСБ и ФСТЭК, юрист компании.

Внутренняя команда будет осуществлять контроль за ходом проекта, привлечением внутренних ресурсов, мотивированием

линейных менеджеров к активному содействию процессу и отвечать за эффективное финансирование проекта. А большую часть работ предстоит выполнить команде консультанта. При выборе подрядчика необходимо оценить следующие аспекты: какой опыт работы имеет данная компания на рынке информационной безопасности, обладает ли она необходимым набором лицензий регулирующих органов (ФСТЭК и ФСБ) для выполнения работ по защите ПДн; может ли компания поставить весь спектр необходимых сертифицированных решений и оказать содействие при аттестации ИСПДн (это требуется для определенных классов систем). Основная цель аттестации – подтвердить, что информационная система ПДн соответствует требованиям руководящих документов по безопасности данных, утвержденных ФСТЭК.

Этапы построения системы защиты ПДн

После того, как в организации сформирована рабочая или проектная группа и выбрана сторонняя ИТ-компания, предстоит последовательно реализовать следующие этапы работы. Прежде всего, нужно определить все ситуации, когда требуется проводить сбор, хранение, передачу или обработку ПДн. Затем – выделить бизнес-процессы, связанные с такими ситуациями. Разумно выбрать ограниченное число бизнес-процессов и проанализировать их. В рамках такого исследования формируется перечень подразделений и сотрудников компании, участвующих в обработке ПДн в рамках своей служебной деятельности. Потом нужно определить круг информационных систем и совокупность обрабатываемых ПДн. Следующий шаг – категорирование ПДн и предварительная классификация ИС. Затем проводится выработка предложений по снижению категорий обрабатываемых ПДн. После этого формируется актуальная модель угроз для каждой ИСПДн, подготавливается задание по созданию требуемой системы защиты. Потом проводится уточнение классов ИС и подготовка рекомендаций по использованию технических средств защиты ПДн. Затем в Роскомнадзор подается уведомление о деятельности в качестве оператора ПДн, а в ФСТЭК – заявка на получение экземпляров руководящих документов по организации системы защиты.

Эти работы предстоит выполнить на первом, начальном этапе. Именно в это время закладывается фундамент успеха всего проекта и делаются основные расходы на консалтинг. Но основная работа происходит на последующих стадиях. Ведь они включают развертывание полноценной производственной системы обработки ПДн, полномасштабное внедрение средств защиты, аттестацию ИС, приведение всех бизнес-процессов обработки ПДн в соответствие с требованиями закона, реагирование на регулярные проверки и т.д.



Евгений Царев,
заместитель директора департамента развития

БАНКОВСКИЕ ТЕХНОЛОГИИ

Журнал «Банковские технологии»
июнь, 2009

Персональные данные. Будни банковской безопасности

Актуальность вопроса защиты персональных данных ни у кого не вызывает сомнений. В первую очередь это обусловлено сроком, определенным для приведения информационных систем персональных данных (ИСПД) в соответствие с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Срок этот неумолимо приближается, и одновременно очевидная сложность выполнения требований руководящих документов регуляторов провоцирует массу споров и неоднозначных трактовок. В то же время закрытость некоторых руководящих документов, их неопределенный правовой статус, как и целый ряд других вопросов, не способствуют решению проблемы. Все это создает ситуацию, когда нормативная база не окончательно определена, а выполнять требования законодательства необходимо уже сейчас. О том, что можно и необходимо делать уже сегодня, рассказывает Евгений Царев, заместитель директора департамента развития LETA IT-company.

Выполнение требований закона для банковского сообщества является вовсе не тривиальной задачей. Здесь есть как организационные, так и технические сложности. Особые проблемы возникают при реализации требований ФСТЭК России. При проведении полномасштабных проектов зачастую возникают неразрешимые ситуации, когда выполнение требований регуляторов равносильно остановке бизнеса. Назрела необходимость выработки компромиссного решения, которое будет учитывать как требования регуляторов (особенно ФСТЭК), так и жизненно важные требования бизнеса операторов персональных данных банковской сферы.

Еще одним очень серьезным аргументом в пользу поиска компромисса с регуляторами можно назвать кадровую проблему. Для банков, как и для других операторов персональных данных, сложилась ситуация, когда отсутствие квалифицированных специалистов становится естественным ограничением при решении задачи создания системы защиты персональных данных. Учитывая, что проблематика защиты персональных данных находится на стыке многих областей знания (право, инженерия, менеджмент и т. д.), найти подготовленных людей по этому направлению практически невозможно. Специалистов нужно учить, а это время и инвестиции. Очевидно, что те 7 млн операторов персональных данных, деятельность которых подпадает под область действия Закона, просто неспособны выполнить тот колоссальный объем работ, который необходимо провести в соответствии с руководящими документами.

Очень активно к поиску путей выхода из сложившейся ситуации для банковского сообщества подключился Банк России в сотрудничестве с Ассоциацией российских банков.

22 мая 2009 г. прошло первое заседание рабочей группы по проблематике персональных данных в АРБ. На мероприятии в ходе открытого обсуждения были вполне четко обозначены проблемные области, волнующие банковское сообщество. В основном они касались именно технической защиты персональных данных и будущего взаимодействия между кредитно-финансовыми учреждениями и ФСТЭК. Представители Банка России озвучили в своем выступлении наработки в части организации исполнения закона «О персональных данных». Принципиально новыми и важными можно назвать попытки Банка России найти компромисс с регуляторами по части формулирования технических требований для банковского сообщества. Особо хочется отметить активность ЦБ РФ в работе с ФСТЭК России. Учитывая всю огромную массу сложностей при выполнении требований руководящих документов ФСТЭК, Банк России принял решение по подготовке собственных документов (проектов документов), которые на сегодняшний день согласуются с ФСТЭК. Можно предположить, что высокая вероятность появления нового отраслевого стандарта для кредитно-финансовых учреждений по персональным данным. Сразу скажу, что предлагаемые ЦБ документы коренным образом отличаются от существующего «Четверокнижия» ФСТЭК.

Что делать сейчас?

Резонный вопрос: что же теперь делать операторам персональных данных? Ведь проверки уполномоченного органа по защите прав субъектов персональных данных уже сейчас идут в массовом порядке, и в плане на 2009 г. стоит более 300 плановых проверок, а есть еще и внеплановые (в 2008 г. количество внеплановых проверок составило 60% от общего числа).

В этой обстановке каждый оператор должен выбрать свой путь: будет ли это комплексный проект, разбиваемый на этапы, либо отдельные «лоскутные» меры и решения.

Если компания выберет второй путь, то сейчас можно сосредоточиться на выполнении требований Роскомнадзора и проведении необходимой аналитической работы, которая не теряет актуальность при возможном изменении требований по технической защите, – в частности, можно сделать следующее:

- подготовить необходимый пакет документов (модель угроз, журналы обращений субъектов и пр.);
- определить, где и какие персональные данные обращаются в организации (выделить ИСПД, классифицировать их и т. д.);
- пересмотреть и доработать договоры с контрагентами на предмет внесения дополнений/исправлений;
- получить согласие на обработку персональных данных от сотрудников и организовать процесс получения согласия от клиентов. ...

Важно понимать, что такой «лоскутный» подход не обеспечивает комплексность проведения работ, не закрывает все тонкие места выполнения требований закона и подзаконных актов. В итоге оператор решит задачу защиты персональных данных лишь частично и не сможет оптимизировать затраты на приведение систем в соответствие с законодательством.

Если компания выберет комплексный проект с привлечением сторонних консультантов, то необходимо внимательно подойти к выбору поставщика услуги, так как далеко не все предлагаемые пакеты услуг позволяют учитывать возможные изменения в нормативной базе, и оптимизировать затраты заказчика. Необходимо, чтобы консультант предложил такой комплекс решений, чтобы не сложилась ситуация, когда вновь созданную систему пришлось бы полностью переделывать под изменившиеся условия через несколько месяцев.

Одним словом, необходимо максимально выполнить требования федерального законодательства и подзаконных актов с учетом возможных перемен.

В чем цель закона «О персональных данных»?

К сожалению, даже специалисты забывают о сути и духе закона. Мы слишком часто сосредотачиваемся на требованиях ФСТЭК и ФСБ России, при этом забывая, что цель закона: «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну».

Закон призван защищать права субъектов персональных данных, и защита информации (по аналогии с законодательством других стран) носит второстепенный характер. Поэтому для любого оператора актуально в первую очередь устранять ситуации, когда нарушаются права субъектов персональных данных. Для этого необходимо:

- наладить работу с обработкой обращений субъектов персональных данных на доступ к своим персональным данным, так как даже несвоевременный ответ на запрос

субъекта является основанием для подачи жалобы в уполномоченный орган по защите прав субъектов персональных данных с последующей внеплановой проверкой;

- наладить работу по удалению/изменению/дополнению персональных данных.

...

Иными словами, необходимо создать систему организационных мер, для адекватного взаимодействия с субъектами персональных данных.

Вместо заключения

Ни для кого не секрет, что за последние полгода ситуация на рынке труда очень сильно изменилась. Одновременно с волной увольнений идет волна исковых заявлений в судах. Федеральный закон «О персональных данных» служит одним из инструментов воздействия на работодателя. Уже есть прецеденты, когда иски в суды несут не с претензиями на «неправильное» увольнение, а с претензиями по обработке персональных данных. Учитывая достаточно жесткие условия и формулировки Закона, сегодня можно выиграть дело практически против любого оператора персональных данных. И опасны здесь не столько материальные потери в виде штрафов, сколько сумма косвенных издержек. Проверка регулятором может занять 4–6 недель, и на это время масса ресурсов компании переключится на обслуживание проверки. Добавьте негативный пример для других сотрудников, повышенное внимание других регуляторов и репутационные риски. В результате получается очень большая сумма издержек, которая может многократно превзойти затраты на построение адекватной системы защиты персональных данных.



Вениамин Левков,
директор департамента
развития



Николай Зенин,
руководитель направления
защиты коммерческих тайн



Журнал «Персональные данные»,
декабрь, 2008

Меры и средства защиты персональных данных

Персональные данные под надежной защитой Symantec DLP

5 ноября 2008 года российское представительство компании Symantec объявило о доступности своих решений Symantec DLP и на российском рынке. Теперь у российских заказчиков появился хороший выбор систем защиты от утечек.

Многие интересуются, каким образом системы **DLP** применимы к требованиям **Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?**

Статья 19 гласит: «Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные

(криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий». Стоит обратить внимание на требование по контролю именно распространения данных. Оператор сам вправе определять технические средства для реализации требований закона. Среди прочих других решений, только подход к защите персональных данных, применяемый в системах DLP, соответствует требованиям практического решения задачи — не допустить неправомерное или случайное распространение персональных данных.

Система защиты от утечек

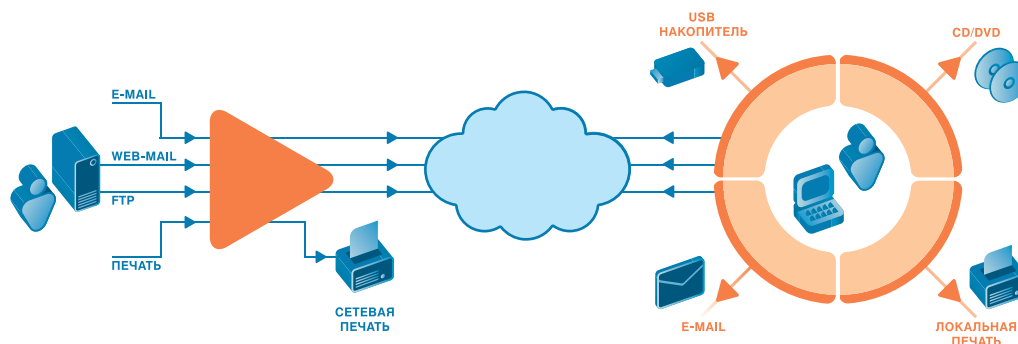
Итак, каково же классическое решение по защите от утечек (DLP), которое предлагает компания Symantec? Рассматриваемая система разрабатывается и постоянно обновляется уже более 8 лет. Независимым аналитическим агентством Gartner решение Symantec DLP признано лидирующим решением по защите от утечек, как по функциональным возможностям, так и по распространенности среди клиентов. В течение 2008 году Symantec DLP было протестировано на корректную обработку русскоязычного контента и уже стартовало несколько проектов развертывания данной системы в российских предприятиях.

Для чего предназначено решение Symantec DLP?

Целью внедрения DLP является, как правило, снижение рисков утечки конфиденциальной информации путем контроля над ее перемещением. Как и любое другое классическое решение класса DLP система выполняет 3 основные функции:

- Мониторинг и контроль перемещения конфиденциальной информации по сетевым каналам связи (email, web, ftp, интернет-пейджеры).
- Контроль действий пользователей на своих локальных рабочих станциях (применительно только к операциям, связанным с отторжением конфиденциального содержимого — на USB-накопитель, запись на диски, через локальные сетевые соединения или печать).
- Сканирование корпоративной сети предприятия (в том числе файловые сервера, порталы, системы документооборота и конечные рабочие станции) на предмет неупорядоченного хранения сведений конфиденциального характера.

Области приложения первых двух функций проиллюстрированы на следующем рисунке:



Каждый сотрудник Вашей компании, обрабатывающий сведения конфиденциального характера, имеющий доступ в интернет и пользующийся корпоративной электронной почтой, способен пересылать информацию не только легитимным получателям, но и себе на домашний компьютер или, что еще хуже, случайным получателям. Система защиты от утечек нацелена на контроль (мониторинг и блокирование) как раз подобных случаев. Таким образом, случайная отправка клиентской базы будет отслежена системой, адресат не получит ожидаемой инсайдерской информации, а в системе DLP будет заведен так называемый «инцидент», который потребует немедленных разъяснений перед службой безопасности.

Конечным результатом работы сотрудника может быть разработанная совместными усилиями проектная документация,

планы работы с перечнем заказчиков. Готовая документация и ее черновые копии могут остаться либо на рабочей станции сотрудника, либо в открытом для всех сотрудников доступе на корпоративном портале. Система DLP обнаруживает места хранения конфиденциальных сведений и выводит отчет о ненадлежащем хранении. Кроме того, наиболее критичные сведения могут быть принудительно перемещены в выделенное место на защищенном сервере. В таком случае, вернувшись на работу после закрытия очередного проекта, сотрудник обнаружит у себя в рабочей области вместо проектной документации ссылку примерно следующего содержания: «В связи с такими-то политиками безопасности, Ваш документ был перемещен в такое-то место на сервере... Вы можете обратиться за разъяснениями к такому-то владельцу данной категории информации».

Модульный состав Symantec DLP.

В соответствии с функциональным подразделением, система делится на несколько модулей, которые могут использоваться как отдельно, так и все вместе:

Функциональная группа	Программный модуль	Способ установки	Краткое описание
Единая платформа интеграции	Enforce Platform	отдельный сервер	Предоставляет доступ к централизованному управлению системой.
Network — обнаружение защищаемой информации в сетевом трафике	Network Monitor	отдельный сервер	Обнаруживает конфиденциальную информацию во всем исходящем сетевом трафике.
	Network Prevent for E-mail	отдельный сервер	Контролирует (возможность блокирования) передачу по email
	Network Prevent for WEB	отдельный сервер	Контролирует передачу через Web (web-почта, форумы, чаты).
Endpoint — контроль операций на уровне рабочей станции	Endpoint Discover	отдельный сервер	Обнаруживает защищаемую информацию, хранимую на локальной рабочей станции
	Endpoint Prevent		Контролирует запись на сменные носители защищаемой информации.
Storage — обнаружение хранимой защищаемой информации	Network Discover	отдельный сервер	Обнаруживает защищаемую информацию, хранимую на файловых серверах, порталах и хранилищах
	Network Protect		Перемещает обнаруженную конфиденциальную информацию.

В качестве типового сервера для развертывания системы используют современное оборудование (2-процессорный сервер с объемом оперативной памяти от 8 Gb).

Как работает Symantec DLP?

Основные преимущества системы DLP перед альтернативными решениями (продуктами шифрования, разграничения доступа, контроля доступа к сменным носителям, архивирования электронной корреспонденции, статистическими анализаторами) — это:

- Осуществление контроля над всеми каналами передачи конфиденциальной информации в электронном виде (включая локальные и сетевые способы), регулярно используемыми в бизнес-деятельности компании.
- Обнаружение защищаемой информации именно по ее содержанию (независимо от формата хранения, каналов передачи, грифов и языка).
- Возможность блокирования утечек (приостановка отправки электронных сообщений или записи на USB-накопители, если эти действия противоречат принятой в компании политике безопасности).
- Автоматизация обработки потоков информации согласно установленным политикам безопасности (внедрение системы не требует расширения штата службы безопасности).

Как же достигается описанный эффект от внедрения DLP-системы? Опишем его на примере одного из основных механизмов детекции — «цифровые отпечатки». Во-первых,

систему подключают к заранее выбранному перечню сведений конфиденциального характера. На предприятии должен быть определен и проклассифицирован перечень той информации, которую следует защищать от утечек. Формат предоставляемой информации может быть в виде текстовых документов, файлов графических форматов, выборок из определенных баз данных. Во-вторых, система обучается на основе предоставленных сведений. С каждого документа снимается набор «цифровых отпечатков» (математические функции, свойственные определенной части содержимого). Причем «цифровые отпечатки» будут сняты как с документа целиком, так с его текстового содержимого и с частей текста. Таким образом, система устойчива к преобразованию форматов и, например, разбавлению части конфиденциального содержимого в открытом тексте. В-третьих, в систему вводятся правила хранения и правила обработки информационных потоков, если в них обнаруживается защищаемая информация. Теперь система настроена и готова выполнять заложенный в нее функционал.

Какие преимущества получает конечный потребитель?

Никому не придет в голову отказаться от установки сигнализации в только что приобретенный автомобиль. Как бы Вы себя почувствовали, если бы вспомнили, что забыли включить сигнализацию в своем автомобиле, припаркованном

на дороге недалеко от входа метро? К сожалению, беспокойства подобного рода одолевают руководителей предприятий, осознающих, что информационные активы постоянно подвержены риску разглашения и попадания в неблагонадежные руки. Как известно, спокойствие стоит дорого, однако для проведения здравого обоснования необходимости системы DLP, следует прибегнуть к оценке рисков. Если совокупная финансовая отдача от использования системы DLP значительно превышает ее стоимость, то, конечно, имеет смысл задуматься над развертыванием системы. На практике, в подавляющем большинстве случаев, эксплуатация систем DLP чрезвычайно выгодна, особенно в пору финансового кризиса, когда многие сотрудники рискуют оказаться на улице. Финансовая отдача исчисляется в виде разницы между уровнем риска (произведение угрозы на ее вероятность) в настоящее время и теоретическим уровнем риска после внедрения системы. Стоимость владения системой Symantec DLP оценивается в \$150-350 тыс. (в зависимости от выбранного набора компонент) в пересчете на каждые 1000 пользователей защищаемых информационных ресурсов.

Каждый день мы используем электронную почту и знаем, что почтовый клиент Microsoft Outlook может предугадывать имена конечных получателей. Он подставляет недостающие символы, когда мы только начинаем заполнять поле адресата. Как часто Ваш почтовый клиент предлагал выбрать не тот адрес? Система DLP отследит, не содержит ли Ваше послание персональных данных, а если и содержит не позволит отправить его ошибочному адресату.

Как часто Вам приходилось ломать голову над тем, разрешены ли к отправке отчет или презентация, которые Вы хотели бы послать Вашему партнеру? Ведь не все конфиденциальные документы промаркированы соответствующим грифом. Система DLP способна проконтролировать и этот вопрос. Используя на своем предприятии систему защиты от утечек, Вам не придется беспокоиться о том, не нарушите ли Вы политику информационной безопасности предприятия.

Особенности работы решения Symantec DLP

Система Symantec Data Loss Prevention обладает поистине широчайшим функционалом, полное описание которого вышло бы далеко за рамки этой статьи. Мы постараемся остановиться лишь на описании наиболее важных функций этого продукта.

I. Контроль записей баз данных

Текстовая информация, содержащая персональные данные (ФИО, адрес, размер зарплаты, e-mail и т. д.) хранится, как правило, в базах данных. Поэтому в первую очередь отметим, что продукт Symantec Data Loss Prevention обеспечивает надежный контроль перемещения такого рода информации за пределы организации.

Общая схема работы следующая:

- записи из определенных столбцов базы данных выгружаются в промежуточный текстовый файл с разделителями;
- этот файл используется продуктом для определения так называемого индекса, по сути, с данных снимается «цифровой отпечаток»;
- этот индекс используется при задании политики контроля, которая определяет ЧТО отслеживается, по КАКИМ каналам и КАК система реагирует на обнаруженный инцидент.

В результате появляется возможность обнаружить информацию из баз данных, например, в приложении к электронному письму, в теле сообщения web-почты или при попытке записи на CD/DVD, а также применить определенные правила реакции. Также отметим, что по опыту работы с системой, при обработке баз данных снимаются более подробные «отпечатки», что позволяет отслеживать даже единичные вхождения.

II. Контроль структурированной информации

В состав персональных данных также очень часто входит информация, имеющая стандартную структуру. Так, определенному формату соответствует номер паспорта, телефона, банковского счета, кредитной карты, ИНН и номер водительского удостоверения. Symantec Data Loss Prevention в состоянии легко отслеживать и такую информацию. Для этого используется механизм регулярных выражений, который позволяет описать формат, например, всех видов данных, перечисленных выше.

С точки зрения настройки системы последовательность действий следующая:

- с использованием стандартного синтаксиса описывается регулярное выражение;
- на его основе задается правило обнаружения, которое включается в политику контроля.

Существующая версия продукта обеспечивает более «жесткую» реакцию на данные, определяемые при помощи регулярного выражения, чем при контроле по «цифровым отпечаткам». Так, при попытке записи подобной информации на съемный USB-носитель, система не только распознает нарушение политики, создаст запись в отчетах и «теневую» копию, но и предотвратит собственно запись информации.

III. Контроль документов

Часть информации, отнесенной к персональным данным, может быть обычным текстом. Описание истории болезни, личное дело, кредитная история — список можно продолжать. Эта информация не имеет какой-то определенной структуры, ее невозможно описать регулярным выражением. На помощь приходит механизм «цифровых отпечатков», позволяющий надежно идентифицировать попытки перемещения документов более 300 различных форматов. Благодаря потрясающей точности «цифровых отпечатков», реализованных в продукте,

удается контролировать не только полный документ, но также его отдельные фрагменты до 10% от общего объема.

Важно также отметить, что объем «цифрового отпечатка» занимает не более 1% от размера идентифицируемого документа.

IV. Комплексный контроль

Одной из важных особенностей продукта является возможность определения комбинированных политик. Все перечисленные выше механизмы контроля, а также условия по ключевым словам, по типу и размеру файлов и еще по многим признакам — все это может использоваться при определении комплексной политики контроля. Причем продукт позволяет реализовать достаточно сложные логические зависимости (OR, AND) между отдельными индексами, по которым ведется поиск конфиденциальной информации. Эта возможность позволяет максимально гибко и эффективно подходить к определению правил контроля для самых сложных случаев.

V. Каналы утечки: сетевые сценарии

Продукт Symantec Data Loss Prevention позволяет отслеживать прохождение информации, определенной в политиках контроля, по любым нешифрованным протоколам стека TCP/IP, включая наиболее распространенные SMTP, HTTP, FTP. Модуль Network monitor интегрируется в сетевую инфраструктуру компании с помощью технологии mirror (SPAN). Т. е. весь трафик, проходящий через коммутатор, зеркалируется на вход Network monitor, который передает полученные пакеты на анализ системе.

Такая схема позволяет вести аудит отправок.

Кроме того, в решение входят два модуля (Network Email Prevent и Network Web Prevent), отвечающих соответственно за блокирование отправок по электронной почте и через web.

VI. Каналы утечки: локальные сценарии

Для контроля локальных сценариев утечки конфиденциальной информации в состав продукта включен модуль Endpoint Prevent. Технически, на конечные рабочие станции устанавливается специальный агент. Его основная задача — контроль и блокирование потенциально опасных действий пользователя. Распределение настроек и политик производится централизованно, со специального сервера в составе комплекса.

Интересно, что агент продолжает сохранять функциональность даже вне сети компании — отключить его рядовому пользователю не под силу. Решение запускает на рабочей станции несколько процессов, которые активируют друг друга при попытке отключения. К слову, в продукте предусмотрены отдельные правила реакции для работы агента при соединении с сетью предприятия и за ее пределами.

Текущая версия продукта позволяет отслеживать копирование данных на съемные USB-накопители, запись CD/DVD, а также на устройства, подключаемые через Firewire и даже iPod. В следующей версии продукта, выход которой запланирован на начало 2009 года, заявлен также контроль печати конфиденциальной информации.

VII. Каналы утечки: перемещение данных на локальную станцию

Интересной возможностью продукта является отслеживание самого факта перемещения конфиденциальной информации на ресурсы рабочей станции с сетевых ресурсов. Для этих целей используется упомянутый выше программный агент. Логика работы следующая:

- при локальном сохранении какого-либо файла агент направляет «теневую» копию этого файла на управляющий сервер Endpoint;
- на сервере снимается «цифровой отпечаток» с этой копии и проводится проверка нарушения активных в этот момент политик контроля;
- в случае их нарушения в единый отчет об инцидентах, который ведется на центральном сервере всего решения, вносится соответствующая запись.

Как видите, даже попытка сохранить данные локально, для дальнейшего манипулирования с ними, может быть обнаружена, причем автоматически.

VIII. Поиск данных в сети

Любая информация, заданная в политиках контроля может быть обнаружена в сети компании с использованием модуля Network Discover. Продукт позволяет обнаруживать данные в сетевых файловых хранилищах, работающих под управлением не только Windows, но и других ОС, таких как UNIX, AIX и Solaris. Поиск ведется также в локальных папках с разделяемым доступом, на порталах Microsoft SharePoint и EMC Documentum, почтовых базах данных, хранящихся на серверах Microsoft Exchange и Lotus, а также в базах данных Oracle, MS SQL, IBM DB2 и на web-серверах.

Во многих случаях обнаруженные данные можно также переместить в сетевой карантин, за что отвечает другой модуль системы — Network Protect. Кроме поиска на разделяемых ресурсах, система позволяет искать данные и в локальных хранилищах. Здесь вновь на помощь приходит программный агент в составе модуля Endpoint Discover и Endpoint Prevent.

Подобный механизм позволит предотвратить попытки бесконтрольного перемещения конфиденциальной информации еще на начальной стадии процесса. Кроме того, сами по себе такие проверки создадут почву для повышения дисциплины работы с конфиденциальной информацией среди сотрудников.

Об авторах

Авторы статьи – ведущие эксперты в области построения систем защиты конфиденциальной информации от утечек. В своей оценке возможностей DLP-решения, представленного в статье, авторы опирались на многолетнюю практику участия в проектах по борьбе с утечками данных. Объективность позиции авторов основана на опыте работы с продуктами практически всех производителей DLP-систем, представленных в России.



Олег Губка,
заместитель директора департамента
развития



Журнал «"Information Security/
Информационная безопасность"», 2009

Фактическая защищенность персональных данных на предприятиях с различной формой собственности

В последнее время тема персональных данных очень активно обсуждается среди специалистов заказчиков и подрядчиков, регулярно проводятся семинары и конференции с участием представителей ответственных органов исполнительной власти, выходят новые статьи по данной тематике. Мало того тема персональных данных стала определенным флагом, под которым пройдет рынок информационной безопасности в 2009 году. В таких условиях, наверное, сложно сказать или добавить чего-то нового. Тем не менее, несмотря на такой повышенный интерес к проблематике персональных данных, обсуждения носят в большей степени теоретический характер. Поэтому в рамках данной статьи я попробую в первую очередь сосредоточиться на практических аспектах удовлетворения требований законодательства по ПДн. Данные практические аспекты не являются интерпретацией соответствующих руководящих документов, а выработаны на основе практического опыта, полученного в рамках проектной деятельности по данной теме.

Опыт реализации проектов по персональным данным показал, что многие компании, несмотря на различный вид деятельности и форму собственности, объединяет определенная похожесть в части процессов обработки персональных данных и обеспечения их защиты. Другими словами среди операторов ПДн можно выделить несколько

типов и дать по ним достаточно четкую оценку, которая позволит более конкретно взглянуть на решение соответствующих задач.

1. Операторы ПДн, которые осуществляют обработку персональных данных только своих сотрудников. Это коммерческие или государственные (в т.ч. муниципальные) организации, которые в рамках своей деятельности не оказывают услуги или не взаимодействуют с физическими лицами. Таких операторов ПДн наверняка будет большинство и можно сказать, что в части удовлетворения требований законодательства по ПДн им повезло больше всех, в прямом смысле этого слова.

Причин такого оптимизма несколько. В первую очередь это определенные «послабления» в рамках организационно-правового поля, а именно непосредственно ФЗ-152. Начнем с получения согласия. В соответствие с требованиями Трудового кодекса любая компания с каждым своим сотрудником подписывает трудовой договор. Это уже является определенной формой согласия на обработку ПДн сотрудника и в соответствие с пунктом 2 части 2 статьи 6 ФЗ-152 дополнительного согласия не требуется. Аналогично можно прокомментировать требование по подаче уведомления о начале обработки ПДн. Так как обработка ПДн ведется в рамках трудовых взаимоотношений, то в соответствие с пунктом 1 части 2 статьи 22 ФЗ-152 оператор вправе осуществлять ее без уведомления уполномоченного органа по защите прав субъектов персональных данных. В этом случае внимание к такой компании или организации со стороны регулирующих органов будет значительно ниже.

В части реализации «технических» требований тоже не возникает серьезных затруднений. Во-первых, для большинства таких операторов это достаточная типовая область работ или объект. В организационном плане это, как правило, 3 вида подразделений, участвующих в обработке персональных данных сотрудников: отдел кадров или персонала, отдел труда и заработной платы, бухгалтерия. Они по-разному могут быть представлены в различных компаниях и организациях, но бизнес-процессы, которые они обеспечивают, остаются практически всегда неизменными.

В техническом плане такой объект чаще всего включает в себя от 10 до 100 рабочих станций, несколько серверов и бизнес-приложения типа 1С, БОСС-Кадровик, SAP HR и другие. Т.е. получается, что область работ, а в конечном счете и ИСПДн, не так глобальна и это далеко не вся компания. Что касается классификации ИСПДн и непосредственно требований по обеспечению защиты ПДн, то здесь зачастую таким системам присваивается 3-й класс, т.к. Хпд=2, т.е. 2-я категория персональных данных, Хнпд=3, т.е. обрабатываются персональные данные субъектов в рамках одной организации. Отсюда все вытекающие последствия/преимущества. Аттестация такой ИСПДн по требованиям безопасности информации не обязательна, а если она еще и локальная, то не надо получать и лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации. В результате вся защита сводится к разработке минимально

необходимого набора документов и внедрению нескольких сертифицированных средств защиты в части соответствующего сегмента сети.

Здесь может возникнуть логичное возражение, что такие компании вряд ли будут озадачиваться решением данных проблем. Не буду приводить теоретических доводов, скажу, что на практике, как не странно, таких заказчиков как минимум не меньше половины. А причин тому несколько. Во-первых с них никто не снимает ответственности за исполнение данного закона, они являются такими же операторами ПДн, в т.ч. с автоматизированной обработкой, а во-вторых затраты на его исполнение получаются вполне посильные. Т.е. результат снижения юридических рисков вполне оправдывает вложенные средства.

2. Операторы, которые обрабатывают персональные данные клиентов. Это компании и организации, которые оказывают услуги и взаимодействуют с физическими лицами. Классические представители данного типа операторов – это банки, страховые компании, негосударственные пенсионные фонды, энергосбыт и т.д. Конечно же, эти компании уникальны в своих процессах обработки ПДн, даже зачастую и в рамках одной отрасли, но есть как минимум один признак, по которому их можно объединить.

3. Это территориальная распределенность. Действительно такие операторы ПДн в процессе своего развития сильно разрастаются географически, пытаются охватить максимальное количество клиентов, которые являются их источником дохода. Причем, несмотря на значительные масштабы компаний, процессы и системы, в т.ч. обработки ПДн, за редким исключением построены по одному стандарту или типу, т.е. достаточно типизированы. Поэтому в рамках проекта по персональным данным нет смысла охватывать сразу всю компанию, а достаточно выделить определенную пилотную зону, в рамках которой эти процессы и системы были бы уникальны, но являлись типовыми в масштабах всей компании.

Такой пилотный проект позволит не только достичь достаточно стандартного преимущества – снижения рисков при масштабировании, – но и значительно снизить затраты, выработав типовые решения (как организационные, так и технические) по защите ПДн, которые относительно легко можно распространить далее.

4. Иностраннные компании. Речь идет о полноценных филиалах зарубежных компаний с образованием юридического лица на территории Российской Федерации. Данный вид операторов не совсем укладывается в рамки выше описанной классификации, т.к. может принадлежать как 1-му, так и 2-му типу, но заслуживает отдельного внимания. Отличительной особенностью таких операторов является то, что довольно часто требования по ИТ и ИБ, «спускаются» из головного офиса за границей.

В связи с этим возникает проблема использования сертифицированных решений по информационной безопасности, как правило, российского производства, в разрез корпоративным стандартам. В такой ситуации можно пойти по пути сертификации существующих средств

защиты, что является весьма длительным и дорогостоящим решением, либо использовать «рядом», не заменяя текущей системы ИБ, сертифицированные продукты с обоснованием перед головным руководством требований местного законодательства.

Также не редко такие операторы осуществляют трансграничную передачу персональных данных, но несмотря на «раздутую» на мой взгляд проблему, на проверку решение данного вопроса является не таким сложным. Действительно, как и многие другие статьи Федерального закона «О персональных данных» статья по трансграничной передаче имеет как часть с обязательным требованием, в частности обеспечения адекватной защиты прав субъектов ПДн, так и часть с исключениями, под которую можно подвести значительную часть процессов обработки ПДн.

Даже если это невозможно, можно опираться на прецедент, связанный с работой соответствующей комиссии Ассоциации российских банков (АРБ). На запрос данной организации был получен официальный ответ от Роскомнадзора с разъяснением пунктов закона, касающихся адекватной защиты прав субъектов ПДн при трансграничной передаче. Данный ответ носит достаточно туманный характер в правовом смысле, но содержит официальное мнение данного органа исполнительной власти, на которое можно опираться при решении спорных вопросов с регуляторами.

С текстом этого письма можно ознакомиться здесь <http://www.arb.ru/site/docs/docs.php?doc=746>.

5. Холдинговые структуры. Здесь под холдинговой структурой понимается совокупность юридических лиц имеющих единую основу и управление, в т.ч. и в вопросах ИТ и ИБ. Типовая проблема в таких компаниях при реализации требований по персональным данным – это то, что каждое юридическое лицо является оператором ПДн, и несмотря на единую инфраструктуру, должно выделить свою ИСПДн и помимо защитных мер подготовить полный комплект документов организационно-правового характера, включая взаимные обязательства по обеспечению безопасности персональных данных при их передаче между юридическими лицами в рамках холдинга. Такую задачу оптимально можно решить, применяя опять же тактику пилотных проектов и дальнейшего масштабирования типовых организационных и технических решений.

В заключение своей статьи, хотелось бы порекомендовать тем операторам, которые находятся в начале пути, не поддаваться панике и не опускать руки в надежде на «авось пронесет», а для начала разобраться в ситуации и провести минимальную оценку возможно даже самостоятельными силами. В результате может оказаться, что масштабы «бедствия» не так велики, вполне посильны и реализуемы.



Илья Новиков,
руководитель направления
информационной
безопасности

iBUSINESS

Издание «iBUSINESS», 2009

Надо ли регистрироваться. Кто сказал, что надо уведомлять Роскомнадзор

«Внимание руководителей государственных и муниципальных органов, предприятий и организаций, индивидуальных предпринимателей, осуществляющих обработку персональных данных! В соответствии со статьями 22,25 Федерального закона от 27 июля 2006 года 152-ФЗ «О персональных данных» организациям, осуществляющим обработку персональных данных, надлежит направить в управление Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия по Мурманской области уведомление об обработке персональных данных» – вот такое пугающее послание обнаружили читатели газеты "Мурманский ВЕСТНИК" от 21.12.2007г., и это не единичный случай подобных требований. Например похожее послание, многие муниципальные образования и организации Республики Башкортостан получили не много ни мало, а со стороны органа государственной власти – Администрации Президента Республики Башкортостан.

После таких грозных посланий мало у какой компании найдется повод подумать, а действительно ли я должен это делать. Помочь разобраться в этом, призвана данная статья.

Так ли это обязательно

По информации публичного доклада руководителя Роскомнадзора – «Реестр создан 31 марта 2008 года. По состоянию на 31.12.2008 г. в него включены 33 697 операторов, осуществляющих обработку персональных данных, из них: государственных органов – 5059, муниципальных органов – 9094, юридических лиц – 19 101, физических лиц – 443».

Возникает вопрос, почему так мало зарегистрировано операторов персональных данных, в то время, как счет тех, на кого распространяется закон, исчисляется миллионами. Фактически можно выделить несколько основных причин

Первая причина – Постоянное изменение формы уведомления и объема запрашиваемых данных. 27 июля 2006 года Федеральный закон №152-ФЗ «О персональных данных» определил, что операторы, которые осуществляют обработку персональных данных, руководствуясь ст.22 закона, обязаны направить в Уполномоченный орган по защите прав субъектов персональных данных (на тот период Россвязьохракультура), соответствующее уведомление не позднее 1 января 2008 года. Идем по хронологии: 11 января 2008 года Россвязьохракультура (предшественница Россвязькомнадзора) утвердила форму уведомления; 22 апреля 2008 года определена методика формирования данных для заявки; 28 марта 2008 года Россвязьохракультура вводит новую форму уведомления; 17 июля 2008 года Россвязькомнадзор (предшественник Роскомнадзора) вводит новую форму уведомления; 18 февраля 2009 года Россвязькомнадзор вносит изменения в приказ о форме уведомления – прошло практически 1 год и 2 месяца с даты определенной в законе. С частыми изменениями формы уведомления у многих зарегистрированных операторов, возникли опасения – Не надо ли будет еще раз подавать уведомление в Роскомнадзор и не придет ли он с проверкой для уточнения недостающих данных?!

Вторая причина – Расхождение между данными уведомления, указанными в №152-ФЗ, и данными в форме уведомления утвержденной Роскомнадзором.

Третья причина – Боязнь попадания в поле зрения контролирующих органов и высокой вероятностью прихода проверки со стороны Роскомнадзора, сразу после подачи уведомления.

Четвертая причина – Неоднозначность требований к организациям, когда необходимо пройти регистрацию в качестве оператора ПДн.

Понимая эти причины, компании фактически нашли для себя три возможных решения данной задачи.

Первая – подождать, посмотреть, что будут делать другие операторы. Если плюсы данной позиции понятны, то минусы упускаются из вида, а они между прочим не так малы, это и то, что в случае проверки к компании предъявят претензии регулятор. Репутационные риски, ведь информация о проверке и выявленные нарушения будут обнародованы на общедоступном сайте соответствующего территориального Управления Роскомнадзора, а ведь ее могу использовать не слишком добросовестные конкуренты. Комиссии может прийти еще много раз проверить насколько вы устранили нарушения, отвлекая от выполнения своих обязанностей и без того занятых Ваших сотрудников.

Вторая – не подавать. Пытаясь найти выход или способы не подавать уведомление. О том, как это можно сделать останавлиюсь подробнее ниже.

Третья – подать. Не важно как, должен я это делать или нет, подать и будь, что будет. На, что стоит обратить внимание компании при формировании уведомления я также останавлиюсь чуть ниже.

Частые нарушения

Итак компания решила для себя, что она будет регистрироваться. С чем она столкнется? Она хочет узнать, как ей правильно подать уведомление и какие данные необходимо в нем указать. Это отнюдь не праздные думы, ведь в законе определено, что вопрос о регистрации может рассматриваться в течении 30 дней, а уведомление о проведении проверки может прийти за 24 часа до нее. И все это время компания чувствует себя крайне незащищенной, тем более, что Роскомнадзор еще ведь и может запросить уточнение или дополнение ранее поданных данных.

Итак, на что стоит обратить внимание

По данным Управление Россвязькомнадзора по Воронежской области одними из главных нарушений, которые встречаются в уведомлении, являются:

- **19% нарушений** – поле «Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных». Операторы не указывают конкретный перечень действий с персональными данными; конкретные способы обработки – неавтоматизированная обработка персональных данных; исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой; смешанная обработка персональных данных с передачей полученной информации по сети или без таковой.
- **17,5% нарушений** – поле «Дата начала обработки персональных данных» Операторы не указывают дату вообще.
- **12,6% нарушений** – поле «Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке». При заполнении данного поля уведомления либо вообще отсутствует описание мер, либо нет их четкого раскрытия.
- **10,4% нарушений** – поле «Цель обработки персональных данных». Необходимо указать как цели, указанные в учредительных документах (уставе, учредительном договоре, положении) оператора, так и цели фактически осуществляемой оператором деятельности.
- **9,9% нарушений** – поле «Категории персональных данных». Операторы зачастую указывают фразы типа «и др.», «и т.п.» «другая информация». Необходимо указывать все конкретные категории.
- **9,2% нарушений** – поле «категории субъектов, персональные данные которых обрабатываются».

Операторы указывают не все категории субъектов, при этом из текста уведомления видно, что обрабатываются данные других категорий.

- **8,9% нарушений** – поле «Правовое основание обработки персональных данных». Операторы не указывают соответствующие статьи и номер закона или иного нормативно-правового акта, регулирующих осуществляемый вид деятельности и касающихся обработки персональных данных.
- **5,8% нарушений** – поле «Срок или условие прекращения обработки персональных данных». Операторы не заполняют данное поле вообще. Необходимо указать конкретную дату или основание (условие), наступление которого повлечет прекращение обработки персональных данных – например «ликвидация юридического лица», «аннулирование лицензии на осуществление соответствующего вида деятельности».
- **5,5% нарушений** – поле «Наименование (фамилия, имя, отчество), адрес оператора».

Типичные ошибки в данном случае:

- не указан (не полностью указан) адрес оператора (например, не указаны почтовый индекс, муниципальный район (для организаций районов области), улица, номер дома, корпус – если имеются), ИНН
- несоответствие полного наименования организации на бланке и (или) печати и в уведомлении. Необходимо точное соответствие.

Кроме этих данных компании в заполнении уведомления помогут изданные Россвязькомнадзором «Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных» Приложение №2 к Приказу №08 от 17 июля 2008 г. Правда, необходимо сказать, что к сожалению они не учитывают требования, которые появились в 2009 г. Но даже в этом случае компании помогут запросы (звонки, письма) в территориальное подразделение регулятора с просьбой разъяснить те или иные сомнительные моменты.

Как не регистрироваться

Теперь давайте рассмотрим другую позицию – как можно избежать регистрации?

Если сформулировать кратко, что надо сделать, чтоб не подавать уведомление, то можно его можно сформулировать так – Все процессы в организации, в рамках которых обрабатываются ПДн, должны быть определены п.2 ст.22 №152-ФЗ.

Да к сожалению это действительно так закон не оставляет другого выхода компании, если она не хочет подавать уведомление. И закон не делает различия между физическими лицами или государственными организациями, если какой-то из процессов выпадает из условий п.2 ст.22 или п.2 ст.1 то организация/компания/физическое лицо обязано подать уведомление.

Если рассмотреть те варианты, под которые необходимо подстроить основные технологические процессы, то их окажется немного:

- обработка ПДн субъектов, которых связывают с оператором трудовые отношения;
- обработка ПДн полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- обработка общедоступных ПДн;
- обрабатываемых ПДн без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн.

Алгоритм же приведение к данным вариантам следующий – Определить технологические процессы обрабатывающие персональные данные; Определить, что за ПДн обрабатываются, от кого получены и на основании чего обрабатываются (Федеральные законы, договора с субъектом, договор со сторонней организацией и т.д.); Сопоставить выявленные процессы обработки ПДн с теми видами обработки, которые позволяют не подавать уведомление (п.2 ст.22 № 152-ФЗ и п.2. ст.1); Определить перечень «отличных процессов»; Определить меры, компенсационного характера, которые позволят привести «отличные процессы» в соответствие (создание общедоступных баз данных, получить соответствующее закону согласие субъекта на распространение/предоставление его ПДн третьим лицам, внести необходимые коррективы в договора с субъектами, проводить обработку ПДн без использования средств автоматизации) и оценить реализуемость этих мер; Провести необходимые компенсационные меры.

Неоднозначность ситуации

Время идет и ранее принятые решения могут меняться, тем более, когда оно принималось в период информационного вакуума, а также неопределенной позицией регуляторов призванных контролировать данный вопрос. Некоторые компании прочитав закон могли решить, что им регистрироваться не надо, а значит не надо проводить каких либо действий чтоб избежать данной участи. Ведь в этом нет нужды. Но на неоднозначность вопроса регистрации в качестве оператора ПДн необходимо остановиться более подробно. В чем здесь заключается загвоздка?

Закон определил несколько основных аспектов, которые сильно влияют на необходимость регистрации компании, это:

- Договор с субъектом ПДн;

- Идентичность цели обработки ПДн, цели определенной в договоре с субъектом/компанией организатором обработки;
- Распространение/предоставление ПДн третьим лицам;
- Обработка персональных данных на основании федерального законодательства.
- И особенности данных условий

Все это хотелось бы продемонстрировать на следующем примере:

В некую компанию X, устраивается на работу гражданин Иванов. При приеме на работу, работодатель запрашивает у Иванова следующую информацию: – Паспортные данные (ФИО, дата и место рождения, место прописки, семейное положение серия и номер паспорта, дата выдачи и кем выдан); Трудовую книжку; ИНН; Карточку пенсионного страхования; Военный билет; Документ об образовании, сертификаты.

Работодателю эти данные необходимы, чтобы начислять Иванову заработную плату, проводить соответствующие отчисления в пенсионный фонд, оформить обязательное медицинское страхование, и т.д. Компания уверена, что т.к. Иванов сотрудник компании, а также обработка его персональных данных осуществляется также во исполнение федеральных законов, то ей подавать уведомление в Роскомнадзор не надо.

С другой стороны, компания X передает их частному охранному предприятию, которое охраняет здание, офис в котором снимает компания, а также вносит данные Иванова в материалы на исполнителей работ, которые передаются сторонним организациям-заказчикам.

Подводный камень кроется здесь в том, что компания X не озаботилась взять согласие Иванова, на передачу его персональных данных охранному предприятию, а в материалы переданных организации-заказчику указала информацию, выходящую за объем информации, разрешенной Ивановым для распространения, это информация о его бывшей работе, его домашний и мобильный телефон.

Все шло хорошо, но Иванова позвали в компанию конкурента и он уволился из компании X. А через некоторое время в компанию приходит внеплановая проверка Роскомнадзора, инициированная письмом от разгневанного Иванова, которому надоела постоянные звонки от представителей организации-заказчика компании X. Комиссия Роскомнадзора, проанализировав ситуацию, нашла все обозначенные выше нарушения, а также нарушение о том, что компания X не зарегистрировалась в качестве оператора персональных данных. Руководитель компании получает соответствующее предписание на устранение нарушений в течении трех рабочих дней, однако выполнить его он не может, т.к. регистрация в соответствии с законом проводится в течение тридцати дней. И вслед за этим на компанию возлагаются новые штрафные санкции. Возможная ответственность ст.19.7 и 19.5 КоАП. Но это не единственные потери компании X, ведь при проверке от выполнения своих должностных обязанностей отвлекаются как

рядовые сотрудники, так и руководство компании, а данные затраты на несколько порядков выше.

Это всего лишь один из возможных вариантов развития событий. Но подумаем, стоит ли компании так рисковать и обеспечивать себе бесконечный сеанс шоковой терапии?

С другой стороны

На самом деле, если рассмотреть те действия, которые, указанная в примере компания, могла выполнить, чтобы к ней не были предъявлены претензии Роскомнадзором о необходимости регистрации, а также помог бы убрать ряд подводных камней, то получилось бы следующее:

- Компания вносит необходимые коррективы в договор с сотрудниками/клиентами компании, затрагивающие вопросы согласия на обработку их персональных данных;
- Компания заключает соглашения с сотрудниками/клиентами компании, в которых определен перечень общедоступных персональных данных и получено письменное согласие сотрудника/клиента на включение его персональных данных в общедоступные источники;
- Компания заключает соглашения с сотрудниками компании/клиентами, в которых определяется перечень персональных данных разрешенных для распространения с указанием компаний получателей и цели передачи персональных данных;
- Компания регулярно проводит контроль информационных систем и документов, хранящих/обрабатывающих персональные данные сотрудников/клиентов, на предмет выявления персональных данных субъектов с которыми закончились договорные отношения и определения необходимости их обработки в соответствии с законодательством (Трудовой кодекс, Налоговый кодекс и т.д.) и при необходимости уничтожения.

Данный перечень можно детализировать и расширять, но вот основные аспекты на которых стоило бы акцентировать свое внимание компании X, если она НЕ хочет подавать заявление на регистрацию.

Как понять по какому пути лучше пойти. Зарегистрироваться или не стоит?

Взвесим, а надо ли регистрироваться

К сожалению, дать однозначного ответа универсального для каждой организации, нельзя. Ведь в некоторых случаях выполнить указанные выше работы является проблематичным и тогда для того, чтобы компании снизить риски санкций со стороны Роскомнадзора, ничего не остается сделать, как подать соответствующее уведомление. Кроме того, данные работы ведь могут расцениваться представителями Роскомнадзора, как подтверждением того, что компания начала выполнять работы по приведению существующих процессов обработки персональных данных в соответствие №152-ФЗ, а значит и

проверяющая комиссия может смягчить санкции за некоторые нарушения.

Но в любом случае, какой бы путь не выбрала организация необходимо понимать, что все эти работы тяжело решить сотрудникам подразделения ИТ или ИБ, т.к. эта задача далеко выходит за рамки типовых. А сбор, например данных о средствах защиты и указание характеристик системы никак нельзя назвать характерными вопросами юридической службы. Так и выходит, что для выполнения данных работ компании вынуждена отвлекать свои лучшие кадры и находиться в неуверенности от правильности принятых решений. А о корректности и полноте сбора и предоставления регулятору данных под гнетом проверки наверное лучше и не говорить. Более логичным видится ситуация, когда компания привлекает стороннего консультанта, который обладает необходимыми знаниями и опытом с тем, чтоб он подсказал, как верно выполнить те или иные работы. Он поможет максимально разгрузить сотрудников компании от выполнения не свойственных им задач, а также оценить и при необходимости реализовать меры по избежанию подачи уведомления. Все это необходимо будет учесть.

Одно лишь можно сказать точно, что из той информации, что доступна по проверкам 2008-2009 г.г., одной из основных претензии у регулятора является не подача компанией уведомления в Роскомнадзор об обработке ПДн. А значит, каждой компании предстоит решить, регистрироваться в качестве оператора персональных данных или провести ряд мер компенсационного характера, которые во многом позволят облегчить жизнь, а также избежать необходимости регистрации.



Николай Конопкин,
заместитель директора департамента
внедрения и консалтинга



Журнал «IT-manager»,
июль-август, 2009

Защита персональных данных: антикризисный подход

2009 год перевалил экватор. Нашему IT-сообществу уже не надо объяснять причины, по которым построение систем защиты персональных данных в компьютерных сетях становится на ближайшее время задачей номер один для всех организаций, в той или иной мере причастных к использованию и обработке персональных данных.

«Проблема 01-01-010» все более уверенно запускает свою жадную лапу в бюджеты операторов, эксплуатирующих информационные системы персональных данных (ИСПДн). Принятие поспешных решений в отсутствие ясного представления о том, какие именно требования должны выполнить операторы, приводит к необоснованному расходу денежных средств.

Нескончаемые исследования хитросплетений федерального закона «О персональных данных», подзаконных актов и руководящих документов ФСТЭК России и ФСБ России с целью нащупать единственно верный путь есть не что иное, как бесполезные траты времени и растущие с каждым днем риски встретить 2010 год с грубейшими нарушениями закона.

Мы продолжаем публиковать рекомендации операторам по

антикризисному решению «Проблемы 01-01-010», основанные на практическом опыте LETA IT-company в проектировании и внедрении систем защиты персональных данных (СЗПДн).

С чего начать?

Звучит банально, но без комплексного предпроектного обследования и составления целостной картины IT-инфраструктуры компании – оператора персональных данных – невозможно сделать ни одного сколько-нибудь обоснованного шага. Тем более, ответить на вопрос о стоимости всего комплекса работ по доведению ИСПДн клиента до полного соответствия требованиям ФЗ «О персональных данных». Вот почему компания, оказывающая услугу по разработке СЗПДн, в начале каждого проекта должна провести «нулевой цикл» первичного изучения объектов внедрения и разработать подробное, детально обоснованное коммерческое предложение на предпроектное обследование. Таким образом, каждый предыдущий этап дает базу для определения стоимости следующего этапа.

Операторы и консалтинговые компании, в зависимости от собственного практического опыта и взгляда на ИСПДн, как правило, применяют при проектировании СЗПДн процессный либо объектовый подход.

Процессный подход дает четкое описание бизнес-процессов, связанных с обработкой персональных данных в информационных системах компании-оператора.

Такое описание технологии обработки ПДн является непременным условием выполнения требований регуляторов. Здесь ИСПДн рассматриваются как совокупности процессов, реализуемых с применением специальных программных средств (автоматизированные системы управления персоналом типа «БОСС-Кадровик», системы «Банк-Клиент», службы каталогов Active Directory, электронные телефонные справочники и др.). Причем, в рамках каждого процесса анализу и описанию подвергается весь комплекс программных и аппаратных средств, обеспечивающих всю совокупность операций и процедур конкретного процесса.

Объектовый подход есть порождение механического следования требованиям регуляторов (прежде всего, ФСТЭК России) к процедуре аттестации ИСПДн. Эти требования вынуждают рассматривать ИСПДн как объекты в четко очерченных границах контролируемых зон: совместно с помещениями, в которых эксплуатируются технические средства, с коммуникациями, проходящими через эти помещения, и разрешительными системами доступа в помещения и к техническим средствам.

Попытки организовать и провести аттестационные испытания ИСПДн как единого целого в совокупности всех систем и в границах всех процессов в масштабе SMB-систем и тем более в

системах масштаба Enterprise обречены на неудачу. Объекты аттестации получают чрезмерно крупными, включающими в себя тысячи приборов, и разбросанными на огромных площадях. Совокупность требований к таким глобальным объектам либо означает прямой путь к созданию СЗПДн с ничтожно коротким временем жизни аттестата соответствия, либо требует несоизмеримо крупных затрат на поддержку в актуальном состоянии, а подчас и вовсе не реализуема на практике.

Именно поэтому наиболее оптимальным является метод суперпозиции процессного и объектового подходов, свободный от подводных камней, подстерегающих нас при чрезмерной приверженности какому-либо одному из них.

Суперпозиция подходов

Суперпозиция процессного и объектового подходов в проектировании заключается в последовательном изучении всех составляющих жизненного цикла каждого из анализируемых процессов в границах каждого из объектов, на которых размещены технические средства, используемые для обработки ПДн.

Как правило, оператор имеет несколько офисов (см. рис. № 1), в каждом из которых реализованы один или несколько технологических процессов (А,В,С...Х), осуществляющих обработку персональных данных. Во всех офисах информация, относящаяся к тому или иному бизнес-процессу и включающая в себя персональные данные клиентов, обрабатывается в одной или нескольких АВС (1,2,3...N). Физическое (с разрывом) или логическое (с применением межсетевых экранов) разделение АВС и АРМ позволяет рассматривать каждую их данных информационных систем как отдельный объект аттестации –

ИСПДн. Размеры контролируемых зон (фактически, границы аттестуемых объектов) сужаются до границ помещений, где размещены технические средства ИСПДн.

На рис. № 1 для наглядности изображена нетипично примитивная ситуация, когда все процессы являются линейными, неразветвленными и непересекающимися (параллельными). В реальности результирующее представление выглядит намного сложнее.

На данном рисунке:

- ИСПДн показаны как совокупности прежде всего технических средств, размещенных в четко очерченных границах контролируемых зон, отделенных от других ИСПДн и внешних сетей средствами межсетевого экранирования. Это соответствует классическому определению ИСПДн, данному федеральным законом;
- в ИСПДн № 1 осуществляются все процессы, связанные с обработкой ПДн, реализуемые в организации. Примером такой ИСПДн служит Главный вычислительный центр, размещенный в центральном офисе холдинга;
- процесс А осуществляется не более чем в одной из ИСПДн каждого из филиалов (ИСПДн 1, 3 и 7);
- процесс С осуществляется не менее чем в одной ИСПДн каждого филиала. Примером такого процесса является перевод заработной платы на банковские карты сотрудников;
- в ИСПДн № 6 осуществляется всего один процесс (процесс Х);
- процесс В в ИСПДн № 7 не осуществляется;
- в каждой ИСПДн используется одна или несколько программных оболочек, соответствующих тем или иным целям обработки персональных данных.

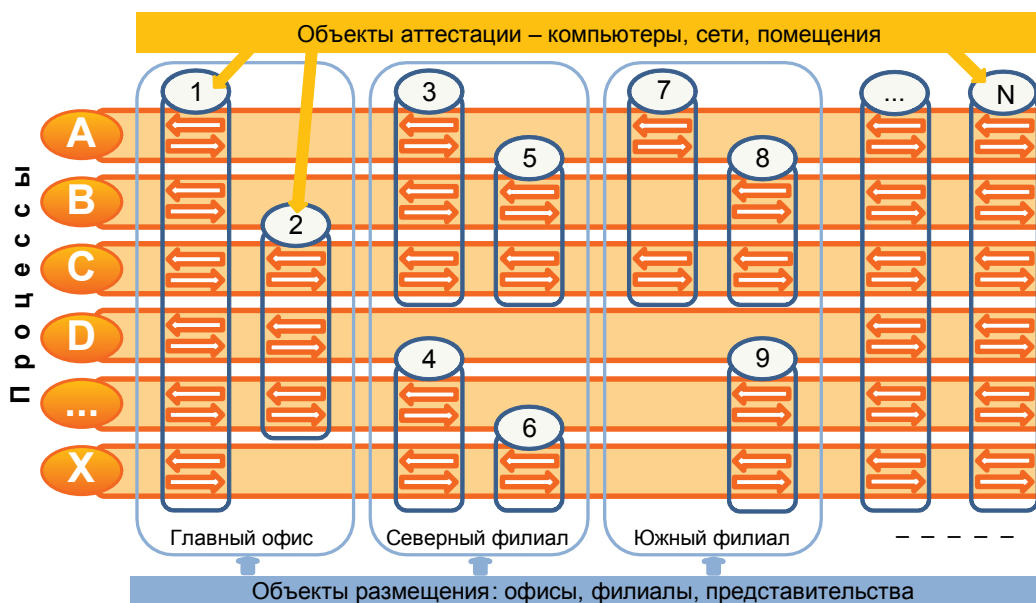


Рис. № 1. Пример суперпозиции подходов

Уже при планировании и расчете стоимости предпроектного обследования подобный подход позволяет получить максимально точное представление об области внедрения СЗПДн и трудозатратах на стадии проектирования.

Суперпозиция подходов при изначально достаточно трудоемкой процедуре предпроектного обследования позволяет многократно экономить ресурсы на последующих стадиях. Прежде всего – за счет разбиения задачи построения комплексной системы защиты персональных данных на серию более мелких задач по подготовке к аттестации нескольких ИСПДн, локализованных в границах четко очерченных контролируемых зон, отделенных друг от друга межсетевыми экранами соответствующего класса и объединенных в единую систему с применением сертифицированных средств криптографической защиты информации.

При этом достигается не только пространственная локализация объекта аттестации, но и исключение из области анализа процессов, не имеющих отношения к конкретной ИСПДн.

Кроме того, выделение в среде аттестуемых ИСПДн однотипных (в нашем случае № 5 и № 8, № 4 и № 9) делает эффективным применение методологии корпоративного стандарта, разработанной и используемой компанией LETA. Данная методология позволяет осуществлять воспроизводство методов защиты, отработанных в пилотной зоне, в остальных сегментах IT-инфраструктуры организации без привлечения сторонних подрядчиков. Это существенно сокращает бюджет всего проекта.

В крупных территориально распределенных информационных системах попытки втиснуть требования к системе защиты для всей IT-инфраструктуры в рамки одного проекта изначально обрекают IT- и ИБ-службы на серьезные проблемы. Применение метода суперпозиции процессного и объектового подходов в проектировании систем защиты, выделение в инфраструктуре сети локальных областей, определяющих общие и специфические требования по защите, разделение на этой основе крупных информационных систем на сегменты, различные по составу применяемых к ним требований, позволяет последовательно концентрировать ресурсы и решать локальные задачи одну за одной.

Именно это определяет особую привлекательность описанного метода для организаций, использующих финансовые затруднения в условиях кризиса и стремящихся в ходе реализации требований ФЗ «О персональных данных» несмотря ни на что сохранить действующие бизнес-процессы и защитить интересы своих клиентов.



Николай Конопкин,
заместитель директора департамента
внедрения и консалтинга



Журнал «IT-manager»,
сентябрь, 2009

Как превратить предприятие в легитимного оператора персональных данных

Что такое класс ИСПДн и каким он должен быть?

Продолжение.

Начало – см. часть 1 от 09.04.2009 г.

Сужение области проектирования систем защиты персональных данных (СЗПДн) до границ локальных информационных систем (ИСПДн) позволяет эффективно использовать возможности по снижению требований к системам защиты до вполне приемлемого уровня. В частности, за счет правильного проведения классификации ИСПДн.

Понижаем класс системы

О снижении класса ИСПДн как способа минимизации требований к системе защиты сказано и написано уже немало, но вопросы у операторов по порядку классификации продолжают возникать. Объяснить суть способа легче с помощью предложенного компанией LETA табличного представления требований «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 г. № 55/86/20 (см. табл. 1).

Характерный пример.

На предприятии работает 5000 человек. В АВС, объединяющей бухгалтерию и отдел кадров, обрабатываются ПДн, позволяющие идентифицировать личность субъекта (паспортные данные) и получить о нем дополнительную информацию (о заработной плате, налоговых и пенсионных отчислениях).

- По количественному признаку коэффициенту ХНПА присваивается значение 2.
- По признаку категории ПДн коэффициенту ХПА присваивается значение 2.
- Наложение признаков даёт значение буквенно-цифрового показателя класса ИСПДн – К2.

Увы, на этом, как правило, и заканчивается процедура определения класса ИСПДн. Казалось бы, класс вполне обоснован, чего же еще?

Увы, при чисто механическом подходе осталось незамеченным, что на самом деле такой системе может быть присвоен более низкий класс. И всего лишь потому, что авторы вышеупомянутого «Порядка проведения классификации...» не удосужились вставить в свой документ специальное упоминание о том, что при присвоении значений коэффициенту ХНПА оператор вправе выбрать любой из определяющих признаков по своему усмотрению.

Достаточно обратить внимание на то, что в приведенном примере в АВС обрабатываются ПДн только сотрудников предприятия, и тут же становится ясно, что коэффициенту ХНПА может быть присвоено значение 3, а ИСПДн – класс К3.

Ситуация меняется кардинально!

Таблица 1. Зависимость класса типовой ИСПДн от категории обрабатываемых данных и количества субъектов, охватываемых системой

Количество субъектов ПДн в системе (Хнпд)	Х _{нпд} = 1			Х _{нпд} = 2				Х _{нпд} = 3	
	Более 100000 ПДн	В объеме РФ	В объеме субъекта РФ	От 1000 до 100000 ПДн	В объеме отрасли	В объеме органа власти	В объеме муниципального образования	До 1000 ПДн	В объеме одной организации
Х _{пд} = 1 Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимной жизни	K1								
Х _{пд} = 2 Данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию				K2					
Х _{пд} = 3 Персональные данные, позволяющие идентифицировать субъекта персональных данных	K2			K3					
Х _{пд} = 4 Обезличенные и (или) общедоступные персональные данные	K4								

Если первоначальное прочтение «Порядка проведения классификации...» вызывает нечто вроде легкого замешательства, то предложенная таблица мгновенно расставляет всё по своим местам.

С понижением класса от K2 до K3 отпадает необходимость в аттестации ИСПДн как объекта, а при отсутствии удаленного доступа к ресурсам – и необходимость получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации. Не говоря уже о том, что в целом совокупность требований к СЗПДн в ИСПДн класса K3 намного легче реализуема. Представленная типовая ситуация с типовой ИСПДн – лишь один из примеров тех путей к снижению класса, которые наглядно демонстрирует нам вышеприведенная таблица.

Это, прежде всего, такие пути, как:

- применение понижающего определяющего признака при установлении значения ХНПД (см. приведенный пример);
- исключение из обработки персональных данных первой категории (ХПД = 1) либо перенаправление процессов их обработки в выделенные специально для этой цели ИСПДн;
- разделение ПДн по категориям и целям их обработки с выделением в особые зоны хранения и обработки данных, определяющих итоговые значения коэффициента ХНПД;
- обезличивание ПДн с выводом информации, содержащей сведения, позволяющие установить однозначную связь между личностью субъекта и его персональными данными, для хранения и обработки в ИСПДн, специально выделенные для этой цели;
- физическое разделение ИСПДн на части при отсутствии производственной необходимости объединения

происходящих в них процессов в случаях, когда такое разделение сопровождается переходом значения ХНПД от 1 к 2 либо от 2 к 3;

- логическое разделение (включая локализацию хранения ПДн) ИСПДн на сегменты с применением сертифицированных средств межсетевое экранирования, обеспечивающее технологический процесс хранения и обработки ПДн, разделяемых по признакам объёма, территориальной либо отраслевой принадлежности, когда такое разделение сопровождается соответствующим изменением значения ХНПД.

Таким образом, при определении класса типовой ИСПДн целесообразно предварительно провести оценку возможности разделения всей ИТ инфраструктуры предприятия на максимально возможное число обособленных сегментов, в каждом из которых обрабатывается минимальное число персональных данных и реализуется минимальное число технологических процессов, связанных с их обработкой. У операторов, озабоченных построением систем защиты персональных данных, есть к регуляторам более серьезный вопрос: как классифицировать информационные системы, относимые к специальным?

Типовая или специальная?

Поток возмущенных вопросов в адрес регуляторов вынуждает их оправдываться, утверждая, что 99% всех ИСПДн по всем параметрам являются «типовыми». Так ли это? И что делать с оставшимся одним процентом ИСПДн, которые к типовым

никак не отнесешь? А ведь это – наиболее критичная их часть! Рискну предположить, что защита именно специальных ИСПДн является важнейшей задачей с точки зрения демонстрации приверженности Российской Федерации Страсбургской Конвенции о защите физических лиц при автоматизированной обработке персональных данных, целям и задачам мирового сообщества по защите прав человека. Обратимся к вышеупомянутому «Порядку проведения классификации...».

Пункт 8 гласит:

Специальные информационные системы – *информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).*

К специальным информационным системам должны быть отнесены:

- *информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;*
- *информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.*

Характеристиками безопасности, «отличными от конфиденциальности», являются целостность и доступность. Это азбука. Однако до настоящего времени не представлено убедительного доказательства безусловного отнесения требований по обеспечению целостности и доступности к персональным данным о состоянии здоровья субъектов. Скажем, в ИСПДн стоматологических поликлиник, школьных медицинских пунктов или страховых компаний.

При наличии записей в медицинских журналах и историях болезней и с учетом юридической значимости данных документов по сравнению с их электронными формами ни целостность, ни доступность электронных форм данных документов не имеет абсолютно никакого значения для субъекта. Возможно, именно на это намекают представители регуляторов, когда рекомендуют рассматривать ИСПДн школ и больниц как типовые? Заметим также, что подобные информационные системы в том же «Порядке...» (см. Таблицу) прямо рассматриваются как типовые ИСПДн (класс К1). Возникает вопрос: как выполнять противоречащие друг другу пункты одного и того же приказа?

«Порядок...» или беспорядок?

Почему не описать в простых и ясных выражениях вышеперечисленные особенности типовых и специальных

ИСПДн в «Порядке проведения классификации...» и дать четкие пояснения по алгоритму классификации тех и других? Вот уж точно: и у трёх «нянек», то есть регуляторов, – «дети без глаза». Однако, какой-никакой, но порядок есть. И мы ему следуем. Предположим, мы установили, что по какому-либо признаку ИСПДн однозначно относится к специальной. Попробуйте хотя бы одному представителю юридического департамента, к примеру, банка или страховой компании доказать, что специальной ИСПДн должен быть присвоен класс, обозначаемый как К1, К2, К3 или К4! Не так-то просто это сделать. Судите сами.

В соответствии с пунктами 14 и 15 «Порядка проведения классификации...» обозначение К1...К4 присваивается лишь типовой ИСПДн. Следующий – пункт 16-й – гласит:

По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

Разве можно трактовать подобную формулировку как достаточное указание на необходимость присваивать специальным ИСПДн такое же обозначение, как типовым? Или, может быть, руководители регулирующих органов, подписывая означенный приказ, искренне верили, что разработанные «в соответствии с пунктом 2 постановления» документы расставят все точки над «ф»?

Как же поступать в подобных ситуациях? Как не допустить ошибки и получить адекватный ситуации Акт классификации ИСПДн?

Специальной системе – специальный класс

Можно сколько угодно критиковать нормативно-правовые акты и методические документы ФСБ России и ФСТЭК России, но нельзя бесконечно выжидать, что проблема исчезнет сама собой. Чересчур поздний старт любого проекта гарантированно приводит к срыву его сроков. С чего-то надо начинать. И нет более правильного пути, чем доскональное исследование ситуации с проблемой защиты персональных данных в компании, идентификация и классификация всех имеющихся ИСПДн в суперпозиции процессного и объектового подходов и составление четко структурированного плана действий до конца 2009 года. Предлагаемый ЛЕТА IT-company алгоритм определения класса ИСПДн удовлетворяет всем возможным пожеланиям самых придирчивых регуляторов и позволяет внести недостающую логику в процесс классификации (см. рис. № 2). Данный алгоритм ориентирован не только на соответствующие пункты «Порядка проведения классификации...», включая пункт 16, но и на методические документы ФСТЭК России, вышедшие позже указанного «Порядка...». Определяющее значение в данном алгоритме имеет разработка Модели угроз, что одинаково необходимо как для специальных ИСПДн, так и для типовых.

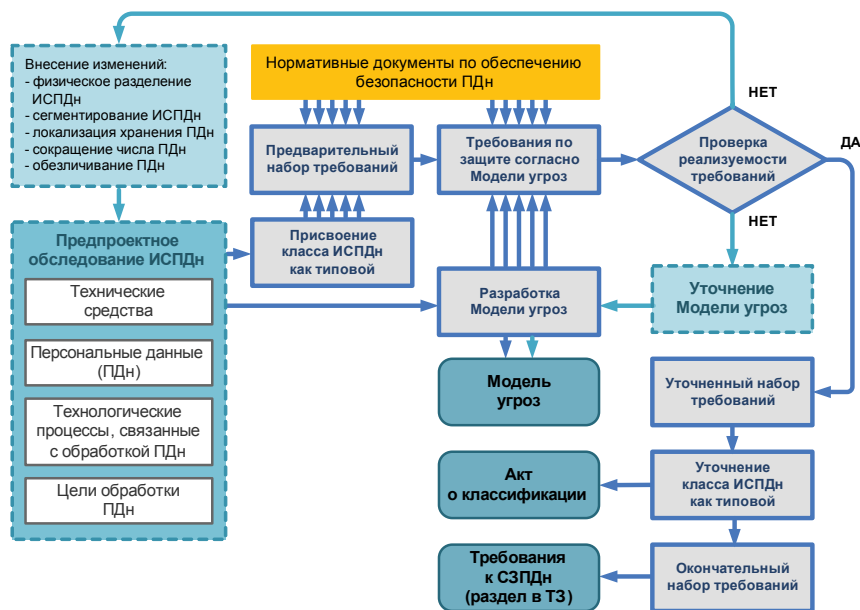


Рис. № 2. Алгоритм классификации ИСПДн

Необходимые исходные данные для определения класса собираются на этапе предпроектного обследования в отдельности для каждой из идентифицированных ИСПДн. На основании результатов изучения перечней защищаемых ресурсов, целей обработки персональных данных и основных параметров технической и программной составляющих ИТ инфраструктуры, условий расположения и других характеристик ИСПДн устанавливаются её классификационные признаки и определяется предварительный класс ИСПДн как типовой.

Одновременно на основе анализа полученных данных и с использованием методических рекомендаций ФСТЭК России и ФСБ России разрабатывается Модель угроз для каждой ИСПДн. Именно здесь особенно внимательного рассмотрения требуют ИСПДн, идентифицированные как специальные. Следующим шагом является определение набора требований к СЗПДн в соответствии с методическим документом ФСТЭК России «Основные мероприятия...».

При этом, как и в традиционной системе базовых принципов и подходов к построению систем защиты, основанной на руководящем документе «Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992 г.), определяющими являются:

- класс ИСПДн как типовой;
- структура ИСПДн (автономная, локальная, распределенная),

- наличие или отсутствие подключения к сетям общего пользования,
- режим обработки (однопользовательский или многопользовательский),
- наличие или отсутствие разграничения прав доступа.

Параллельно на основании тех же нормативных актов по обеспечению безопасности ПДн формируется набор требований к СЗПДн, направленных на предотвращение угроз безопасности, актуальность которых установлена в результате разработки модели угроз.

Общий набор требований проходит оценку их реализуемости. На результаты оценки могут повлиять как технические особенности той или иной ИСПДн и наличие или отсутствие подходящего набора сертифицированных средств защиты, так и требования неизменности реализуемых бизнес-процессов, не говоря уже о финансовых возможностях организации.

В случае отрицательного результата оценки вместе либо по отдельности включаются механизмы:

- доведения ИСПДн до состояния, в котором предъявляемый к ней набор требований будет полностью реализуем (прежде всего механизмы снижения класса, описанные выше). Данные механизмы включаются и применяются один за другим либо в комплексе, и в итоге должны привести к положительному результату оценки применимости требований к СЗПДн;

- введения ограничений в модели угроз. Данный метод может потребовать как проведения серии специальных измерений и расчетов, так и согласования получаемых моделей угроз с регулирующими органами. Его целесообразно применять в том случае, если механизмы корректировки ИСПДн не привели к ожидаемому результату.

При наличии положительного результата оценки применимости требований к системам защиты разработанные модели угроз утверждаются как окончательные. Организация получает первый из обязательных для разработки пакетов документов. Уточненные наборы требований по защите сравниваются к предварительными наборами требований, предъявленными к ИСПДн как к типовой.

Внимание!

Весьма важно не упустить из виду возможные ситуации, когда для реализации уточненного набора требований необходим уровень защиты, превышающий требования к предварительно определенному классу системы как типовой. В этом случае первоначально установленный буквенно-цифровой показатель класса может быть пересмотрен в сторону повышения.

В частности, типичной является ситуация, когда утечка информации по каналу побочных электромагнитных излучений из технических средств и наводок на провода и линии, выходящие за пределы контролируемой зоны (ПЭМИН), в типовой ИСПДн класса К2 представляет настолько серьезную угрозу, что требуется дополнительное применение специальных сертифицированных средств защиты от утечки по каналу ПЭМИН. А это характерно уже для ИСПДн класса К1. Акты классификации ИСПДн составляют второй пакет обязательных для разработки на данном этапе документов. Итоговое представление Акта классификации ИСПДн включает в себя все перечисленные в «Порядке проведения классификации...» классификационные признаки.

Третий пакет составляют окончательные наборы требований к СЗПДн. В них включаются не только требования к подсистемам защиты от несанкционированного доступа, межсетевое экранирование, антивирусной защиты и др., но и требования к системе управления безопасностью, включая организационно-режимные требования, а также требования по аттестации и лицензированию. Окончательные наборы требований формулируются в виде отдельных документов либо в качестве разделов в отчеты и могут служить основой для разработки технического (частного технического) задания на систему защиты в целом. В традиционной системе руководящих документов ФСТЭК России акт классификации автоматизированной системы (АС) уместается на одной странице и заканчивается краткой формулировкой типа: Класс, присвоенный системе: 1Г.

При составлении Акта классификации ИСПДн итоговая формулировка класса выглядит такой же сложной, как сам алгоритм ей вывода. Например:

- **Класс, присвоенный системе:** специальная, распределенная, имеющая подключение к сетям международного информационного обмена, многопользовательская с разграничением прав доступа, расположенная полностью в пределах Российской Федерации, по значению последствий нарушения заданной характеристики безопасности для субъектов персональных данных соответствующая типовым ИСПДн класса К2, требующая дополнительных мер защиты (К2+).

Различия в итоговых формулировках очевидны.

Возвращаясь к истокам

Дело в том, что АС классифицируются только по требованиям защиты информации от несанкционированного доступа. Прочие классификационные признаки АС разбросаны по целому ряду руководящих документов (СТР-К и др.). Все они используются при формировании окончательного набора требований к системе защиты АС без усложнения первого документа, разрабатываемого при проектировании системы защиты – Акта классификации. При разработке «Порядка проведения классификации...» и методических документов по защите персональных данных традиционные методы установления взаимосвязи между характеристиками информационной системы и требованиями к системе защиты, разбросанные по множеству руководящих и нормативно-методических документов, механически и недалековидно сведены в одно целое. Именно поэтому предписанный для использования порядок классификации ИСПДн получился таким громоздким. Сталкиваясь с проблемами уже на этапе разработки планов приведения своих информационных систем в соответствие с требованиями ФЗ «О персональных данных», операторы не решаются сделать следующий шаг и либо занимают выжидательную позицию, либо впадают в юридическую казуистику. Сравнение итоговой формулировки класса ИСПДн с традиционной формулировкой класса автоматизированной системы и первые опыты применения методических документов ФСБ России и ФСТЭК России при проектировании систем защиты персональных данных дают понимание того, как много надо еще сделать, чтобы разработанные на скорую руку методические документы регуляторов и описанные в них подходы к построению систем защиты персональных данных перестали вызывать недопонимание и неприятие у операторов.

О LETA IT-company

LETA IT-company (www.leta.ru) – первый российский оператор типизированных ИТ-услуг, обеспечивающий заказчикам комплексные решения в области информационной безопасности. Спектр услуг LETA IT-company включает все этапы жизненного цикла построения информационной безопасности на предприятии – аудит, консалтинг, внедрение, сопровождение.

В линейку услуг LETA IT-company входят как инновационные (защита персональных данных, оценка защищенности сетевых ресурсов и внедрение систем управления уязвимостями и т.д.), так и классические ИБ-услуги (защита информации от инсайдеров и предотвращение утечек конфиденциальных данных – DLP, построение систем ИБ по российским и международным стандартам и т.д.).

Ведущие позиции LETA IT-company на рынке ИБ подтверждает ряд достижений:

- 3 место в рейтинге «CNews Security 2007: крупнейшие ИТ-компании России в сфере защиты информации» (2008 год);
- 1 место в рейтинге CNews «Защита информации и бизнеса от инсайдеров» (2007 год);
- победа в номинации «Системы и средства защиты информации» программы «Лучшие инновационные решения в области технологий безопасности 2007 г.» по итогам международного форума «Технологии безопасности 2007» (2007 год);
- награда «Лучшее решение в области информационной безопасности 2007» от Microsoft (2007 год).

В ходе оказания услуг LETA IT-company взаимодействует с 40 ведущими зарубежными и российскими разработчиками, в рамках технологических партнерств с которыми обладает 30 авторизованными статусами различного уровня, в частности:

- Platinum Partner от Symantec,
- Gold ChannelConnect Partner от Websense,
- Premier Partner Solution Provider от McAfee,
- AffinityPlus Partner от Trend Micro,
- Bronze Partner от Check Point,
- Gold Certified Partner от Microsoft (с компетенцией «Security Solutions» в числе других)

и т.д.

LETA IT-company входит в состав LETA Group – управляющую компанию в сфере передовых информационных технологий, наряду с LETA IT-company объединяющую компании MrSoft («Мистер Софт»), ESET («ИСЕТ»), «Дамаск», АСК, Veyer.

Свяжитесь с LETA IT-company по вопросам защиты персональных данных, обрабатываемых в Вашей организации

Контакты авторов:

Вениамин Левцов,
Директор департамента развития
VLevtzov@leta.ru

Илья Новиков,
руководитель направления
информационной безопасности
INovikov@leta.ru

Евгений Царев,
заместитель директора департамента
развития
ETsarev@leta.ru

Николай Зенин,
руководитель направления
защиты коммерческих тайн
NZenin@leta.ru

Олег Губка,
заместитель директора департамента
развития
OGubka@leta.ru

Николай Конопкин,
заместитель директора департамента
внедрения и консалтинга
NKonopkin@leta.ru

Контакты LETA IT-company:

109129, Москва, ул. 8-я Текстильщиков,
д. 11, стр. 2

Тел./факс: +7 (495) 921 1410
e-mail: info@leta.ru
<http://www.leta.ru>

