Частные вопросы управления ИТ-инраструктурой

**Особенности управления ИТ-инфраструктурой в условиях правоприменении законодательства в области работы с персональными данными**

Вступление в силу Федерального Закона №152 «О персональных данных» привело к необходимости значительно пересмотреть состав и организационные решения по управлению ИТ-инфраструктурой на большинстве предприятий. Закон и подзаконные акты предусматривают строго регламентированную процедуру приведения информационных систем персональных данных (ИСПДн) в соответствие законодательству.

**Законодательная база организации работы с персональными данными**

*Конституция РФ*. В соответствии со статьей 23 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

*Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и защите информации»*. Создает правовые, организационные и экономические основания для реализации права на свободный поиск, получение, передачу, производство и распространение информации.

*Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных».* Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов 80 Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

*Постановление правительства РФ № 781 от 17.11.2007 г.* *«Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».* Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

*Постановление правительства РФ № 687 от 15.09.2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».* Настоящее положение определяет особенности организации обработки персональных данных и меры по обеспечению безопасности персональных данных при их обработке, осуществляемых без использования средств автоматизации

*Приказ ФСТЭК РФ № 55, ФСБ РФ № 86 от 13.02.2008 г. и Мининформсвязи РФ № 20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».* Настоящий Порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

*Приказ Россвязькомнадзора № 8 от 17.07.2008 г. «Об утверждении образца формы уведомления об обработке персональных данных» (с изменениями от 18.02.2009 г.).* Настоящим приказом определен, рекомендуемый к использованию при направлении уведомления об обработке персональных данных, образец формы уведомления, а также даны рекомендации по его заполнению.

*Приказ ФСТЭК РФ № 58 от 5.02.2010 г. «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».* Настоящее Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных.

*Методический документ ФСТЭК РФ «Базовая модель угроз безопасности персональным данным при их обработке в информационных системах персональных данных» от 15.02.2008 г.* Данный документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. В модели угроз дано обобщенное описание информационных систем персональных данных как объектов защиты, возможных источников угрозы безопасности персональных данных, основных классов уязвимостей информационных систем персональных данных, возможных видов деструктивных воздействий на персональные данные, а также основных способов их реализации.

*Методический документ ФСТЭК РФ от 15.02.2008 г. «Методика определения актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных».* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

**Классификация ИСПДн**

Основаниями для классификации ИСПДн являются:

* Категория обрабатываемых в информационной системе персональных данных - Хпд;
* Объем обрабатываемых персональных данных - Хнпд;
* Характеристики безопасности персональных данных, обрабатываемых в информационной системе;
* Структура информационной системы;
* Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
* Режим обработки персональных данных;
* Режим разграничения прав доступа пользователей информационной системы;
* Местонахождение технических средств информационной системы.

По категории ПДн делятся на:

* категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
* категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
* категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
* категория 4 - обезличенные и/или общедоступные персональные данные.

По объему ПДн выделяют три объема:

1. в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта РФ или РФ в целом;
2. в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования; 84
3. в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

По характеристикам безопасности ПДн выделяются:

* Типовые ИСПДн – требуется только конфиденциальность данных.
* Специальные ИСПДн - требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий). К специальным ИСПДн в любом случае относятся: o информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных; o 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.

По структуре ИС можно выделить следующие типы ИСПДн:

* автономные (не подключенные к иным информационным системам) комплексы технических и программных средств;
* комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
* комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

**Особенности управления ИТ-инфраструктурой в условиях использования свободного программного обеспечения**

Понятие свободного ПО было введено **Ричардом Столлменом** для поддержки научного сообщества в области разработки ПО на принципах совместной научной работы. В основе этого понятия четыре критерия свободного ПО, они же четыре свободы

1. Программу можно свободно использовать с любой целью
2. Можно изучать, как программа работает, и адаптировать её для своих целей. Условием этого является доступность исходного текста программы.
3. Можно свободно распространять копии программы — в помощь товарищу.
4. Программу можно свободно улучшать и публиковать свою улучшенную версию — с тем, чтобы принести пользу всему сообществу.

Одна из первых свободных лицензий, которая появилась еще на заре операционных систем и универсального ПО – **лицензия BSD**. Эта лицензия очень простая и обладает минимумом ограничений. Фактически она заботится только об охране честного имени автора:

* Разрешается повторное распространение и использование как в виде исходного кода, так и в двоичной форме, с изменениями или без, при соблюдении следующих условий:
* При повторном распространении исходного кода должно оставаться указанное выше уведомление об авторском праве, этот список условий и последующий отказ от гарантий.
* При повторном распространении двоичного кода должна сохраняться указанная выше информация об авторском праве, этот список условий и последующий отказ от гарантий в документации и/или в других материалах, поставляемых при распространении.
* Ни название, ни имена ее сотрудников не могут быть использованы в качестве поддержки или продвижения продуктов, основанных на этом ПО без предварительного письменного разрешения.

Одной из наиболее распространенных сегодня лицензий на свободное ПО является лицензия GNU's not Unix General Public License. В ее основе лежат собственно свободы Столлмена. Эта лицензия декларирует следующее:

* Право на копирование и распространение исходного кода.
* Право на изменение исходного кода при соблюдении условий:
* Требование добавления информации об изменениях в модифицированных файлах.
* Требование лицензирования модифицированных версий под той же лицензией.
* Возможность по требованию вывода информации об авторских правах и отсутствии гарантии
  + Требование предоставления исходного кода (на выбор): o Исполнимый код распространяется вместе с исходным.
  + Исполнимый код распространяется вместе с гарантией предоставления исходного по требованию.
  + То же с гарантией от третьей стороны.
* Лицензия прекращает действие при любом ее нарушении.
* Указание перечня актов, обозначающих принятие лицензии.
* Запрет на дополнительные ограничения при распространении.
* Невозможность внешних ограничений изменить требования лицензии. То есть независимость от законодательства – твой закон противоречит лицензии – не используй продукты под этой лицензией.
* Отказ от гарантий и ответственности.



**Особенности управления ИТ-инфраструктурой с точки зрения информационной безопасности на основе стратегии Microsoft Trustworthy Computing**

Концепция защищенных компьютерных построена на четырех принципах:

* безопасность, которая предполагает создание максимально защищенных ИТинфраструктур;
* конфиденциальность, которая подразумевает внедрение в их состав технологий и продуктов для защиты конфиденциальности на протяжении всего периода их эксплуатации;
* надежность, которая требует повышения уровня надежности процессов и технологий разработки программного обеспечения информационных систем;
* целостность деловых подходов направлена на укрепление доверия клиентов, партнеров, государственных учреждений.

Для решения вопросов обеспечения информационной безопасности компания Microsoft предоставляет следующие технологии:

* Active Directory – единый каталог, позволяющий сократить число паролей, которые должен вводить пользователь;
* двухэтапная аутентификация на основе открытых/закрытых ключей и смарт-карт;
* шифрование трафика на базе встроенных средств операционной системы IPSec (IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов);
* создание защищенных беспроводных сетей на основе стандарта IEEE 802.1x;
* шифрование файловой системы;
* защита от вредоносного кода;
* организация безопасного доступа мобильных и удаленных пользователей;
* защита данных на основе кластеризации, резервного копирования и несанкционированного доступа;
* служба сбора событий из системных журналов безопасности.

**Механизм управления групповыми политиками**

Для компьютеров, входящих в домен Active Directory, используются групповые политики, определяющие политики безопасности, используемые в рамках сайта, домена или набора организационных единиц (OU – organizational units). Групповые политики и Active Directory позволяют:

* централизованно управлять пользователями и компьютерами в масштабах предприятия;
* автоматически применять политики информационной безопасности;
* понижать сложность административных задач (например, обновление операционных систем, установка приложений);
* унифицировать параметры безопасности в масштабах предприятия;
* обеспечить эффективную реализацию стандартных вычислительных средств для групп пользователей.

Применение групповых политик и Active Directory для сайтов, доменов и организационных единиц необходимо реализовывать с учетом следующих правил:

* объекты групповой политики (GPO) хранятся в каждом домене индивидуально;
* с одним сайтом, доменом или организационной единицей может быть сопоставлено несколько GPO;
* с несколько сайтов, доменов или организационных единиц могут использовать единственную GPO;
* любому сайту, домену или организационной единице можно сопоставить любую GPO;
* параметры, определяемые GPO, можно фильтровать для конкретных групп пользователей или компьютеров на основе их членства в группах безопасности или с помощью WMI-фильтров.

При администрировании ИТ-инфраструктуры предприятия администраторы посредством механизма групповой политики могут производить настройку приложений, операционных систем, безопасность рабочей среды пользователей и информационных систем в целом. Для этого используются следующие возможности:

* политика на основе реестра. С помощью редактора объектов групповой политики можно задать параметры в реестре для приложений, операционной системы и её компонентов;
* параметры безопасности. Администраторы могут указывать параметры локальной, доменной и сетевой защиты для компьютеров и пользователей в области действия GPO, используя шаблоны безопасности;
* ограничения на использование программ. Данные ограничения предназначены для защиты от вирусов, выполнения нежелательных программ и атак на компьютеры;
* распространение и установка программ. Обеспечивается возможность централизованного управления установкой, обновлением и удалением приложений;
* сценарии для компьютеров и пользователей. Данные средства позволяют автоматизировать операции, выполняемые при запуске и выключении компьютера, при входе и выходе пользователя;
* мобильные пользовательские профили и перенаправление папок. Профили хранятся на сервере и позволяют загружаться на тот компьютер, где пользователь входит в систему. Перенаправление папок позволяет размещать важные для пользователя папки на сервере;
* автономные папки. Данный механизм позволяет создавать копии сетевых папок, синхронизировать их с сетью и работать с ними при отключении сети;
* поддержка Internet Explorer. Эта возможность позволяет администраторам проводить управление конфигурацией Microsoft Internet Explorer на компьютерах с поддержкой групповой политики

**Управление авторизацией и аутентификацией пользователей**

Инфраструктура открытых ключей **PKI (public key infrastructure)** – это системы цифровых сертификатов, центров сертификации CA (certification authorities) и других центров регистрации RA (registration authorities), которые идентифицируют (проверяют подлинность) каждой стороны, участвующей в электронной транзакции, с применением шифрования открытым ключом (public key). **Службы сертификации (Certification Services)** и средства управления сертификатами позволяют построить предприятию собственную инфраструктуру открытых ключей.

* более устойчивая к взлому защита, которая базируется на аутентификации с высокой степенью защищенности и применении смарт-карт, использовании протокола IPSec для поддержания целостности и защиты данных от попыток несанкционированной модификации при передаче по общедоступным сетям, а также использовании шифрующей файловой системы для защиты конфиденциальных данных, хранящихся на сервере;
* упрощение администрирования за счет создания сертификатов, которые позволяют избавиться от применения паролей, масштабировать доверительные отношения в рамках предприятия;
* дополнительные возможности, которые обеспечивают безопасный обмен файлами и данными между сотрудниками предприятия по общедоступным сетям, защищенную электронную почту и безопасное соединение через Web;
* использование сертификатов, которые представляют собой цифровой документ, выпускаемый центром сертификации и подтверждающий идентификацию владельца данного сертификата;
* службы сертификации, которые применяются при создании и управлении центрами сертификации;
* шаблоны сертификатов, которые представляют собой набор правил и параметров, применяемых к входящим запросам на сертификаты определенного типа;
* автоматическая подача заявок на сертификаты, которая позволяет администратору конфигурировать субъекты сертификатов для автоматического запроса сертификатов, получения выданных сертификатов и возобновления просроченных сертификатов без участия их субъектов;
* Web-страницы подачи заявок на сертификаты, которые позволяют подавать заявки на сертификаты через Web-браузер;
* политики открытых ключей, которые позволяют автоматически распространять сертификаты их субъектам, определять общие доверяемые центры сертификации и проводить управление политиками восстановления данных;
* поддержка смарт-карт, которая позволяет обеспечивать вход в систему через сертификаты на смарт-картах, хранение на них сертификатов и закрытых ключей

**Управление защитой коммуникаций**

Для защиты коммуникаций предназначена технология IP-безопасности, базирующаяся на протоколе IPSec (IP Security). В корпоративной информационной системе данная технология должна обеспечивать защиту от:

* изменения данных при пересылке;
* перехвата, просмотра и копирования данных;
* несанкционированного изменения определенных ролей в системе;
* перехвата и повторного использования пакетов для получения доступа к конфиденциальным ресурсам

**Безопасность мобильных пользователей корпоративных систем**

Для безопасной работы мобильных пользователей используются следующие виды защиты:

* защита домена;
* защита мобильного устройства;
* защита беспроводных соединений.

Для защиты беспроводных соединений сетевые администраторы должны контролировать процесс доступа этих устройств к корпоративной сети предприятия. Кроме того информация, передаваемая по беспроводной сети должна шифроваться.

SSL – протокол шифрованной передачи данных между клиентом и сервером, который требует сертификата, выданного одним из авторизованных центров. TLS — криптографический протокол, который обеспечивает безопасную передачу данных между узлами в сети Internet. SSL, используя криптографию, предоставляет возможности аутентификации и безопасной передачи данных через Internet. Часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным.

Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытых ключей SSL включает в себя три основных фазы:

* диалог между сторонами, целью которого является выбор алгоритма шифрования;
* обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификата;
* передача данных, шифруемых при помощи симметричных алгоритмов шифрования.

Для корректной работы аутентификации SSL (TLS) удаленные клиенты должны:

* работать под управлением Windows 2000 или Windows XP;
* использовать клиент протокола RDP (Remote Desktop Protocol);
* доверять корневому сертификату сервера