Защита конфиденциальной информации при работе информационных систем в государственных организациях остается важной прикладной задачей. В типовом российском государственном структурном подразделении в перечень конфиденциальных сведений входит многочисленная рабочая документация, значительная часть входящей и исходящей корреспонденции, рабочие записи и личные дела сотрудников компании, образцы некоторых документов и др.

В последнее время системы обеспечения безопасности документооборота считаются приоритетными для современных офисов. При этом этапы "начальной" и "финишной" обработки документов, содержащих конфиденциальные сведения, являются довольно уязвимым звеном общего процесса документооборота. Каналы ввода и вывода информации в этом контексте являются наиболее уязвимыми, так как именно через эти потоки конфиденциальная информация (как полученная извне, так и порожденная внутри организации) соединяется с авторами и потребителями. Слабая защищенность таких каналов способствует вторжениям, особенно внутренних нарушителей. Действительно, в течение рабочего дня значительное количество конфиденциальных документов копируется, размножается, печатается, докладывается руководству, переделывается, сканируется, пересылается по каналам электронной почты и многие аналитики вполне логично признают, что проблему защиты информационных ресурсов именно от внутренних нарушителей широко используемые специализированные средства разграничения доступа пользователей к информационным ресурсам не решают. Связано это со следующими тремя основными факторами:

* внутренний нарушитель является авторизованным пользователем, следовательно, ему легче осуществлять несанкционированные действия;
* внутренний нарушитель находится в среде обладателей и носителей конфиденциальной информации, активно общается с ними, в том числе по каналам Intranet, где информация объективно менее контролируется;
* внутренний нарушитель легально получает доступ и работает с конфиденциальной информацией, следовательно, существует возможность записи ее на внешние носители, печати, сканирования и последующей обработки при отсутствии должного контроля.

Активно развиваемая в бизнесе концепция так называемой "персонализации печати" (private printing) ставит задачу учета личных особенностей потребителей информации и приобретения возможности соответствующим образом оперативно "настраивать" свои системы печати. С развитием таких масштабных проектов как "Электронная Россия", "Электронная Москва" и др. вопросы "персонализации" печати конфиденциальной информации будут приобретать все большее значение.

Наличие ограничений на процессы обработки конфиденциальной информации существенно ограничивало до недавнего времени применение современных офисных устройств для их обработки. Однако появление специальных многофункциональных офисных устройств, способных одновременно выполнять многочисленные функции по обработке документа (сканирование, копирование, печать, финишная обработка и др.), предоставило дополнительные возможности по обработке конфиденциальной информации. Широкому внедрению таких устройств способствовал переход от аналоговых к цифровым способам обработки информации. Действительно, однократно осуществив "оцифровку" информации, ее затем можно многократно использовать. Но здесь кроется и определенный "подводный камень". Увеличивается количество каналов и простота перехвата такой информации, большее количество исполнителей имеет доступ к местам ее хранения и др. Все это усложняет задачу обработки конфиденциальной информации.

Можно выделить несколько основных направлений защиты информации при ее вводе в корпоративные сети и выводе из них:

* зашифровка информации при передаче конфиденциального задания на печать или копирование и расшифровка ее непосредственно перед началом процесса;
* максимальное ограничение доступа к процессам распечатки/копирования конфиденциального документа;
* обеспечение защиты от несанкционированного доступа к уже изготовленному и содержащему конфиденциальную информацию документу;
* уничтожение конфиденциальной информации после ее обработки и изготовления документа без возможности восстановления.

По некоторым оценкам, в настоящее время из-за нерациональной организации документооборота европейские компании каждый год теряют порядка 98 млрд. евро. При этом потенциал офисных технологий реализуется всего на 70%. И "львиную" долю потери этого потенциала составляет слабо продуманный и неавтоматизированный документооборот, в составе которого и процессы ввода и вывода документов.

В российских госструктурах традиционно используются следующие организационные меры защиты:

* установка соответствующей офисной техники в закрытых помещениях, доступ в которые ограничен и контролируется;
* реализация правил разграничения доступа к устройствам создания твердых копий;
* закрытие доступа к портам печати; для вывода конфиденциальной информации на "твердую" копию необходимо вызвать администратора, который разрешит печать конфиденциальной информации;
* наличие и поддержание в актуальном состоянии разнообразных по форме и содержанию списков контроля доступа;
* развитые средства протоколирования событий, происходящих в системе при обработке документа;
* использование для печати конфиденциальных документов персональных принтеров, подключенных непосредственно к компьютерам сотрудников, допущенных к работе с такой информацией и др.

К наиболее существенным элементам программного обеспечения безопасности в государственных структурах относится так называемое мандатное управление доступом. Здесь для каждого пользователя устанавливается определенный уровень допуска к конфиденциальной информации. Каталогам или файлам назначается категория конфиденциальности. Доступ к файлу пользователь получит только в том случае, если его уровень допуска не ниже уровня конфиденциальности файла.

Сотрудники соответствующих служб многих государственных структур полагают, что таких функций достаточно, чтобы выявить несанкционированное копирование конфиденциальной информации или ее распечатку, а также узнать, кто из пользователей превышает ограничения, установленные политикой безопасности. Вместе с тем, такие организационные меры являются необходимыми, но не достаточными для обеспечения безопасности на завершающих этапах обработки конфиденциальной информации.

Внимательный анализ используемых методов и средств показывает, что большинство мер направлено на защиту все же от внешних, а не внутренних нарушителей. Необходимо считать внутреннего нарушителя "…специалистом высшей квалификации, который знает все об автоматизированной системе и, в частности, о системе и средствах ее защиты…". Так, специалист, имеющий доступ к жесткому диску, потенциально может извлечь конфиденциальную информацию, уже подготовленную для печати или иной обработки. Пользуясь возможностями внутренней электронной почты, внутренний нарушитель может перенаправить документ или его обезличенную часть по неустановленному адресу. Возможна реализация и иных угроз.

В последнее время появляются решения, удовлетворяющие как требованиям по оперативной и качественной обработке документов, так и требованиям по безопасности ее обработки и представления. Многие западные поставщики разрабатывают специальные классы многофункциональных аппаратов для компаний и организаций с высокими требованиями по обработке информации с высоким уровнем конфиденциальности, таких как правительственные структуры, подразделения ведомств, имеющих отношение к обороне, служб безопасности, банков, юридические и производственные фирмы и др. При этом в ряде случаев обеспечению функций безопасности при разработке офисных устройств придается высочайший приоритет.

Наиболее общие подходы таковы.

1. Решения, как правило, предполагают наличие некоторых технических средств и клиентского программного обеспечения, инсталлируемого непосредственно на компьютерах авторизованных пользователей.
2. Материалы, отправленные на печать, защищаются паролем и не распечатываются до тех пор, пока исполнитель не введет пароль, либо с дисплея печатающего устройства, либо удаленно со своего терминала.
3. Временные данные, которые сохраняются после выполнения любой операции на аппарате в памяти, стираются способом, не допускающим восстановления.
4. Задания при отправке на печать зашифровываются и расшифровываются непосредственно перед печатью.
5. Обращения к печати разрешаются только с тех компьютеров, адресам которых присвоены соответствующие полномочия.
6. Предусматривается автоматическая сортировка выводимых документов по персональным ячейкам сотрудников, физически закрываемых на ключ.

Для обеспечения безопасности предусматриваются и меры обеспечения безопасности: наличие малозаметных точек при печати, печать на фоне логотипа предприятия, с учетом места расположения и др.

Стандартные возможности также достаточно разнообразны:

* выход финишных копий, отпечатанных или откопированных документов в МФУ "изображением вниз";
* автоматическая сортировка выводимых документов по персональным ячейкам сотрудников;
* наличие промежуточных электронных "почтовых ящиков" пользователя, в которых можно сохранять электронные копии документов;
* задержка выполнения задания на печать до тех пор, пока пользователь не идентифицирует себя с помощью пароля на каком-либо из сетевых принтеров;
* специальные алгоритмы принудительного уничтожения информации с жесткого диска внутри аппарата после печати/копирования без возможности ее восстановления "специальными" методами;
* сканирование непосредственно на сервер электронной почты (scan-to-email);
* направление отсканированных документов с панели управления аппарата на компьютер конкретного пользователя в заданную папку (scan-to-folder).
* автоматическая блокировка создания нежелательных дубликатов какого-либо документа;
* специальное программное обеспечение - так называемые наборы защиты данных, устанавливаемые на устройство ввода-вывода и компьютеры и защищающие информацию комплексно. Программы позволяют производить печать конфиденциальных документов при условии идентификации пользователя, а также имеют гибкие возможности по разграничению прав сотрудников на использование тех или иных печатающих устройств посредством специальных идентификационных устройств.

В зависимости от предпочтений Заказчика, класса выполняемых задач, желаемой степени закрытости чувствительной информации и особенностей работы у отдельных решений можно найти определенные конкурентные преимущества перед остальными, которые в той или иной ситуации могут стать и определяющими.

Естественным и объективным критерием для выбора решения должен быть критерий "эффективность- стоимость". Необходимо выбирать решение, обладающее минимальной суммарной стоимостью владения при удовлетворении требований по оперативности и качеству печати и выполнении основных требований по безопасности. При этом в качестве основного критерия при выборе целесообразно использовать "цену отпечатка". В этом критерии в консолидированном виде отражаются все основные характеристики многофункциональных устройств, в том числе одна из основных составляющих совокупной стоимости владения – стоимость расходных материалов. Так, например, если цена отпечатка меньше всего на $0.02, то совокупная стоимость владения аппарата в своем классе на протяжении, например, 5-7 лет эксплуатации, окажется на 10-15 % меньше, чем эта характеристика других аппаратов.

В качестве примера применения современных возможностей по выполнению таких важных для обработки конфиденциального документа функций, как сканирование, печать и копирование, рассмотрим многофункциональные офисные устройства торговой марки NASHUATEC.

В таких аппаратах реализованы все важнейшие функции, необходимые при работе с конфиденциальной информацией - временные данные на жестком диске стираются без восстановления посредством специальной функции, можно заблокировать печать документа и распечатать его при введении своего пароля с панели управления в присутствии исполнителя, выделенные файлы могут быть блокированы для нежелательных пользователей, при наборе неправильного пароля файл для печати блокируется и др.

Кроме того, можно выделить еще ряд интересных и новых подходов.

Учет разнообразных условий обеспечения и выполнения требований по безопасности в крупных организациях часто становится отдельной непростой задачей, особенно значимой для администраторов по безопасности и пользователей. Так, например, пользователю становится необходимым помнить (или записывать!) разнообразные уникальные логины и пароли авторизации доступа к различным устройствам – компьютерам, офисному оборудованию, учитывать ограничения, налагаемые для различных групп клиентов и др. В указанных выше устройствах не требуется запоминание дополнительных паспортов, идентификаторов для пользователей, традиционных кодов доступа к сетевому оборудованию. Имена пользователей и пароли, вводимые при стандартной авторизации WINDOWS используются и для "входа" в многофункциональное устройство.

Нестандартное решение получено и на стыке обработки результата с учетом необходимости его последующей отправки пользователям. Использование электронного документооборота в организациях, обрабатывающих конфиденциальную информацию, существенно сдерживается сложностью контроля ее обработки и пересылки по каналам электронной почты. В частности, практика работы с конфиденциальной информацией потребовала исключить возможность подделки поля "От" к шаблоне письма электронной почты при реализации функции scan-to-email (сканирование с последующей отправкой по каналам электронной почты). И теперь авторизованное имя пользователя автоматически поступает в поле "Имя отправителя" и изменить его нельзя. Таким образом, отсканированный материал отправляется только в заданный адрес и недоступен при сканировании другим пользователям.

Специальная политика ограничения управления передачей файлов ограничивает доступ к файлам во время их передачи. Только пользователи, которым даются соответствующие полномочия, могут переправить файл в иное место после сканирования. Для затруднения исключения доступа внутренних нарушителей к обрабатываемой информации реализована также функция "Сканирование в папку".Иными словами, информация по завершении сканирования будет направлена непосредственно в папку данного пользователя на его рабочей станции, минуя каналы электронной почты и др. Такая функция существенно сужает круг лиц, работающих с конфиденциальной информацией.

*Четыре главных функции политики управления файлами и доступа к приложениям:*

* ограничение возможности работы с документом (например, только чтение);
* редактирование документа при печати – пользователь может читать и изменить установки печати);
* расширенное редактирование - пользователь может редактировать установки печати и уничтожать файлы, предназначенные для печати;
* полный контроль – пользователь выполняет все указанные выше функции и может администрировать права других пользователей (напечатать файл, задержать его печать, просмотреть контент и информацию и др).

По существу, обеспечивают высокую степень гибкости администрирования процессов обработки документов. Не требуется даже специальных администраторов по безопасности; обычный администратор компьютерной сети может поддерживать и функции администрирования офисного устройства.

Ограничению доступа к информации, которая может быть значимой для внутреннего нарушителя, способствует решение о специальном кодировании адресной книги, в которой аккумулируются сведения обо всех зарегистрированных лицах, допущенных к работе на данном аппарате.

В целом положительными характеристиками является высокая гибкость комплексного решения, которая при непосредственном применении существующей структуры в процессах обработки конфиденциальной информации исключает несанкционированное использование аппарата, ограничивает доступ к любому или нескольким (всем) приложениям, облегчает работу системного администратора и, в целом, является очень удобной в практическом применении.

Таким образом, на рынке офисной техники предлагается множество разнообразных решений, удовлетворяющим требованиям по безопасности обработки информации на этапах ее входа в защищенную систему и выхода из нее. Они предназначены для работы с цифровыми многофункциональными устройствами в таких структурах, как правительство, силовые ведомства, крупные корпорации и др. Высокие эксплуатационные характеристики таких аппаратов могут стать ключевыми для совершенствования процессов документооборота в государственной структуре, обрабатывающей конфиденциальную информацию.