perimetrix

КОММЕРЧЕСКАЯ ТАЙНА

О ДЕЙСТВЕННОЙ ЗАЩИТЕ ПРОЕКТНОЙ ДОКУМЕНТАЦИИ

Фильмы об ограблениях начинаются с того, что мошенники покупают проектно–строительную документацию на объект грабежа. Причём продаёт им документацию обычно сотрудник самой организации, прекрасно понимающий, что эта документация будет использована против интересов его организации. Очевидно, что банальный подкуп намного проще и эффективнее подготовки шпиона или штурма извне. Для нас важно, что сюжеты фильмов зачастую берутся из реальной жизни.

Но есть и ещё один вопрос, о котором менеджеры проектных подразделений производственных компаний не хотят говорить. Производственные площадки перенасыщены опасными объектами, вся информация по ним сосредоточена в проектных архивах. И если ваши люди учатся правильно проектировать аммиакопроводы, хранилища хлора и ГСМ, то где–то относительно недалеко другие люди учатся их правильно уничтожать. Всё что им нужно — ваш чертеж, чтобы точно знать куда заложить взрывчатку.

Поэтому политика руководителя проектного подразделения «меня эта безопасность не касается, моё дело — выдавать ПСД в срок» — это близорукая политика. И запоздалое «а меня–то за что?» никогда не находит понимания ни у вышестоящего руководства, ни у работников прокуратуры.

Предотвратить нельзя поймать

Практически каждая проектно–конструкторская или архитектурно–дизайнерская фирма в той или иной степени сталкивается с задачей предотвращения утечек своих наработок «на сторону». Часто в беседах с проектантами мы слышим горестные рассказы, как на тендерах в конкурирующих предложениях «всплывают» их собственные чертежи или проекты. Время потрачено, вложены силы и средства — и в последний момент выясняется, что «ноу–хау» компании уже совсем не «ноу–хау», тендер проигран, а компания теряет не только долгожданный контракт, но и уникальные наработки и конкурентные преимущества.

«Массовые расстрелы» не исправят ситуацию, и надо искать «брешь», через которую утекли важные данные. Зачастую руководитель компании в таких случаях начинает «свирепствовать» и волевым решением запрещает все, что только можно — флешки, локальные принтеры, выход в Интернет, электронную почту, Skype и пр. В результате ломаются привычные в компании рабочие процессы, процедуры обмена данными, падает продуктивность работы, снижается трудовой настрой — и вместо решения одной проблемы фирма получает массу других.

Что делать? Как найти разумный баланс между «закручиванием гаек» и борьбой с утечками? Кого привлечь к поиску «брешей»?

Современная проектно–конструкторская документация — это сложный информационный продукт, создаваемый коллективно средствами автоматизированного проектирования, поэтому естественно возникает мысль — нужно обратиться за помощью к ИТ–специалистам, которые устанавливают и обслуживают САПР. Однако в таком решении есть подвох, о котором руководитель фирмы даже не подозревает.

Кадры решают: «Ой, всё!...»

Для того, чтобы понять, почему ИТ — это не та служба, которая может до конца бороться за безопасность информации, необходимо понять основную мотивацию ИТ–шника.

С точки зрения информационной безопасности, тремя основными свойствами информации являются доступность, целостность и конфиденциальность. При этом в непосредственные задачи ИТ–службы, как подразделения, обслуживающего основной бизнес компании, входят прежде всего обеспечение постоянной доступности ИТ–сервисов и обеспечение их целостности (корректности). Задача же обеспечения конфиденциальности, т.е. разграничения доступа к информационным объектам, требует от ИТ–шника доскональных знаний о содержимом обрабатываемых данных, об их бизнес–ценности для компании, о полномочиях сотрудников в части доступа к тому или иному информационному контенту — то есть о тех «материях», о которых осознанно может судить лишь «владелец» этих

данных — главный конструктор, руководитель проектного отдела, финансовый директор и пр. Другими словами, ИТ–шник просто не обладает достаточными знаниями для принятия оперативных текущих решений для обеспечения нужной степени конфиденциальности. В такой ситуации ИТ–шник либо «бьет по площадям», вводя общие ограничительные правила «для всех», либо старается переложить решение о классификации информационного контента на людей, способных реально оценивать важность обрабатываемых данных.

Кроме того, ИТ–шнику мировоззренчески сложно внедрять защитные средства, затрудняющие и ограничивающие пользователям доступ к информационным ресурсам, ведь основная задача ИТ — обеспечивать как раз доступность ИТ–сервисов. Информационная безопасность зачастую понимается ИТ–шником как обеспечение безопасности не информационного контента, а безопасности самой ИТ–инфраструктуры — т.е. антивирусная защита, резервное копирование, устранение уязвимостей базового программного обеспечения, контроль доступа в Интернет и пр.

Отсюда следует несколько важных выводов. Во–первых, решение о выборе средств защиты информационных активов компании (ее ноу–хау, проектно–конструкторских и архитектурно–дизайнерских наработок) должно приниматься не ИТ–службой, а руководителями, ответственными за безопасность бизнеса, с привлечением специалистов, обладающих необходимой подготовкой в области информационных технологий. Во–вторых, в классификации информационных активов безусловно должны участвовать линейные руководители подразделений, которые лучше, чем кто–либо, понимают ценность создаваемой и обрабатываемой информации как для самой компании, так и для конкурентов, которые хотят ее заполучить.

Анатомия утечки

Вернемся теперь вновь к проблеме утечек и попробуем понять, как они происходят. Давайте проанализируем, как происходит создание и перемещение информации при создании сложного информационного продукта, каковым является проектно–конструкторская и архитектурно–дизайнерская документация. Хотя информация «невещественна» и «неосязаема», в каждый момент она находится в каком–то виде в определенном месте — «информационном контейнере». Таким «контейнером» может быть мозг конструктора, файл на диске или флэшке, электронное письмо, распечатанный на принтере чертеж или CAD–овское приложение, в котором работает конструктор. При обработке информация перемещается из одного контейнера в другой: например, «пояснительная записка к проекту» из головы проектировщика вносится в память офисного приложения Microsoft Word, затем сохраняется в файл на жестком диске компьютера, откуда может быть отправлена по электронной почте, скопирована в сетевую папку, распечатана на принтере и т.д. В каждом случае мы видим перемещение информационного объекта из одного контейнера в другой. При этом способов таких перемещений множество. Информация в электронном виде приобрела такую «текучесть», которой она не обладала в докомпьютерную, «бумажную» эпоху. Утечка — это цепочка последовательных «элементарных» перемещений, в результате которых наша ценная информация оказалась в руках тех, кому она не предназначена.

Первое, что приходит в голову, когда встает задача обеспечения защиты информации — это поставить ограничительные барьеры на всех каналах связи, через которые информация может «утекать», и на этих барьерах попытаться успеть проанализировать, разрешено ли этой информации покидать периметр организации, или нет. Программные средства защиты должны уметь отличать «легитимные» перемещения от «нелегитимных», блокируя неразрешенные действия и пропуская разрешенные. Фактически такие средства должны анализировать весь трафик, на ходу разбирая и классифицируя контент.

Поскольку основной задачей при этом становится определение «запретных» перемещений, то в систему должно вводиться множество признаков, по которым защитная система должна определять «неразрешенное» действие. Анализируется контекст, шаблоны, цифровые отпечатки, типы файлов и т.д. и т.п. Правила определения «запрещенного перемещения» должны анализировать все возможные способы (протоколы) передачи информации, отлавливая «подозрительную» информацию. При этом в погоне за зловредным нарушителем важно не заблокировать ложными срабатываниями нормальный производственный процесс,

поскольку потери от простоев могут превысить возможный ущерб от утечки. В результате, компании вынуждены применять подобные средства лишь в режиме «зеркалирования» или мониторинга, сохраняя результаты сработки правил в архив для последующего «разбора полетов». Фактически, утечка все равно происходит, и мы узнаем о ней с запозданием. Правда, в системе остается след и есть возможность расследования инцидента и выявления виновного.

Не было у папы заботы...

И тут компания сталкивается с очередной проблемой! Расследование инцидента информационной безопасности должно привести к каким—то последующим действиям — внесению новых правил распознавания «запрещенного перемещения» и наказанию виновного. Для того, чтобы наказать виновного, предъявив ему доказанный факт нарушения внутренних правил, компании необходимо подготовиться «по всем фронтам» — разработать и прописать положения режима коммерческой тайны, внести соответствующие изменения в трудовые договоры, ввести процедуры ознакомления сотрудников «под роспись» с материалами, содержащими коммерческую тайну, создать и оформить внутреннюю комиссию, которая будет разбирать подобные инциденты, и т.д. и т.п. «Руководство пользователя» информационной системы предприятия превращается в огромный список запретов, которые сотрудник, если и изучит до конца, то в реальной жизни наверняка забудет и не станет исполнять.

Зачастую на этом месте руководитель уже опускает руки, понимая, что ввязавшись за борьбу с утечками, придется перерабатывать существующие и разрабатывать новые регламенты, привлекать и оплачивать дополнительную работу кадровиков и юристов, обучать сотрудников и требовать с них исполнения новых правил. Поэтому внедрение режима коммерческой тайны часто останавливается лишь на декларировании наличия такой тайны у организации и написании положения «О коммерческой тайне», но не перерастает в регулярный работающий процесс.

Где же выход из этого унылого круга? На самом деле выход есть, и он достаточно простой, нужно только поставить проблему «с головы на ноги».

В защиту режима

Давайте посмотрим на задачу защиты важной информации с точки зрения руководителя организации. Он не задумывается о сетевых протоколах, портах ввода—вывода, адресах сетевых хранилищ, допустимых расширениях имен файлов и т.д. и т.п. Это все — «излишние материи». Руководитель никогда не станет досконально и по пунктам определять, что «нельзя» делать с важной информацией. Он говорит — «Делаем так, как я сознательно разрешил. Делают те, кому я разрешил. Все остальное в отношении наших информационных активов, вредное, ненужное и необязательное — приказываю решительно пресечь».

Таким образом, старый демократичный подход к защите по принципу «Разрешено все, кроме того, что запрещено» меняется на кардинально противоположный — «Запрещено все, кроме того, что в явном виде разрешено». Несмотря на кажущуюся категоричность этой максимы, подобный подход к защите по—настоящему важной информации существенно более продуктивен, чем его либеральная противоположность.

Во—первых, правильных, «разрешенных» рабочих процессов в компьютерной среде на порядок меньше, чем всех возможных. Разрешенные рабочие процессы заранее известны, более стабильны и менее вариативны. Поэтому список «разрешенных» процессов составить гораздо проще, чем описать все, «что нельзя».

Во—вторых, описывая и закрепляя «разрешенные» рабочие цепочки, мы стандартизуем и упорядочиваем их, что в конечном итоге приводит к увеличению их эффективности и безопасности.

В—третьих, построенная таким образом схема защиты никак не мешает правильным (разрешенным, легитимным) действиям пользователей, поскольку строится именно вокруг них.

Чтобы реализовать подход «Запрещено все, кроме того, что в явном виде разрешено» на уровне информационной системы, нам необходимо сделать четыре последовательных шага.

Дорогу осилит идущий

Шаг первый → *классификация* контента. Нужно определить предмет защиты и степень его важности для компании.
Шаг второй → *полномочия* (допуски)

наших пользователей по работе с этим контентом.

Шаг третий → определение *правил* (на языке ИТ—«*политик*»), согласно которым наши пользователи будут работать с классифицированным контентом.

Шаг четвертый → *внедрение* системы, которая будет на каждом шаге сверять полномочия пользователей с классификационными признаками обрабатываемой информации и разрешать или запрещать последующее действие.

Давайте рассмотрим все вышесказанное применительно к проектно—конструкторской деятельности. Определимся, что предметом защиты являются чертежи, создаваемые в CAD—приложениях, сопутствующие им текстовые документы, таблицы, рисунки и др., создаваемые в офисных приложениях и все вместе хранимые на каких—либо PDM—порталах.

Любой документ из вышеперечисленных снабжается неотъемлемой «классификационной меткой», которая сопровождает его и все производные документы, созданные на его основе, на всех этапах их «жизненного цикла», и определяет допустимые для него программы обработки, места хранения, способы передачи.

Классификацию информации можно и нужно выполнять в понятных бизнесу категориях, в соответствии с таким уровнем детализации, который обеспечит необходимую гранулярность в полномочиях пользователей.

Например, ❶ можно задать следующие *измерения*:

— Конфиденциальность (значения: «несекретно», «ДСП», «коммерческая тайна»);

— Функциональность (значения: «конструкторские данные», «дизайн», «финансы», «маркетинг»).

❷ пользовательские *полномочия* определяются в тех же нотациях, например:

- **Главный конструктор** имеет доступ к «конструкторским данным» любой степени секретности, а к прочим данным только до уровня «ДСП»;
- **Экономист** имеет доступ только к «финансовым данным» с признаком «секретности» — «несекретно» и «для внутреннего использования»;
- **Секретарь** имеет доступ к документам с любой функциональностью, не относящимся к «коммерческой тайне»;
- **Генеральный директор** имеет доступ ко всему.

❸ Когда мы определяем *политики* работы с данными, мы можем формулировать их на достаточно высоком уровне, например:

- Конструкторские данные могут *храниться* только на сервере PLM/PDM—системы и жестких дисках авторизованных компьютеров.
- *Обработка* КД возможна только с использованием определенных политиками приложений (AutoCAD, Компас, NanoCAD и пр).
- *Печать* конструкторской документации разрешена только на определенных сетевых принтерах, находящихся в отделе выдачи проектов.
- Разрешено *копирование* КД и ДД только на учтенные съемные накопители и в определенные сетевые папки.
- *Отправка* КД по электронной почте разрешена лишь на утвержденный список адресов.
- *Хранение* КД в «облачные» хранилища не описано, как разрешенное.

Затем эти политики транслируются в низкоуровневые политики системы защиты, и проверка легитимности перемещений информационных объектов отслеживается иконтролируется уже на уровне элементарных перемещений из одного «информационного контейнера» в другой.

Автоматизация защиты

Сразу возникает вопрос — кто, как и когда будет проставлять эти классификационные метки? Не придется ли пользователю все время помнить об этих метках и выполнять дополнительную работу? Что будет, если пользователь неосознанно или, наоборот, сознательно не проставит метку? Ответ простой. «Львиную часть» работы по проставлению меток, также как и по контролю перемещений информации, выполняет сама защитная система. Пользователь — лицо для системы «недоверенное», т.к. мы как раз хотим защитить нашу важную информацию от его нелегитимных действий.

Реализуется так называемая **мандатная модель доступа**. «Владелец данных» определяет ценность данных и основные требования по обеспечению их безопасности, а пользователь лишь оперирует данными в строгом соответствии с правилами (*политиками безопасности*). Даже при создании информации

пользователь не принимает решения о выборе метки, за него это делает система в соответствии предписаниями «владельца данных».

Поэтому метки проставляются следующим образом: первоначальная классификация информации, хранимой на рабочих компьютерах пользователей, выполняется специальным модулем защитной системы, которая сканирует места хранения и по заданным правилам (типу файла, контексту, месту хранения и т.д.) присваивает файлу определенную классификационную метку, с которой он будет жить в дальнейшем. Например, можно определить также правило, что любому новому файлу, создаваемому в Автокаде будет автоматически присваиваться метка «Коммерческая тайна, Конструкторские данные». Все дальнейшие действия с таким файлом будут впредь подчиняться установленным политикам безопасности. Более того, если пользователь сделает копию этого файла, метка «наследуется» и второй экземпляр файла также будет «помечен». Метка неотрывно следует за информационным контентом не только при копировании файла, но и при перемещении контента в буфер обмена, при передаче в другое приложение и т.д. Можно реализовать более сложные процедуры присвоения меток, например, если конструктор получает информацию для дальнейшей работы из PDM—портала, то можно установить правило, по которому такая информация «на лету» будет получать определенную классификационную метку.

Как быть в ситуации, когда по смыслу рабочего процесса необходим вынос контролируемой информации за пределы защищаемого периметра? Например, если нам необходимо показать проект заказчику в его офисе? В таком случае предусматривается помещение информации в «криптоконтейнер», представляющий собой своего рода зашифрованный архив. Открыть такой криптоконтейнер можно только на ноутбуке с установленным драйвером защиты и при наличии канала доступа к серверу корпоративных политик, который и выдает пароль для открытия криптоконтейнера. Таким образом, даже вне офиса на контролируемую информацию будут распространяться корпоративные политики безопасности.

Левак не пройдет

Одним из приятных «кейсов» применения описанной схемы защиты является борьба с «леваком». Не секрет, что некоторые проектировщики ухитряются в течение оплачиваемого рабочего дня рисовать проекты для своих «левых» заказчиков. Компания теряет на этом порой значительные деньги, оплачивая рабочее время, которое используется проектировщиком «не по назначению». Так вот, устанавливая классификационные метки и описывая разрешенные процедуры, мы делаем невозможным «вынос» результатов «халтуры» за пределы организации любым иным путем, кроме как через корпоративный отдел выдачи.... «Левак» теряет смысл, потому что результаты такой работы уже нельзя вынести за пределы организации, не признавшись в ее выполнении в рабочее время corporate channels.

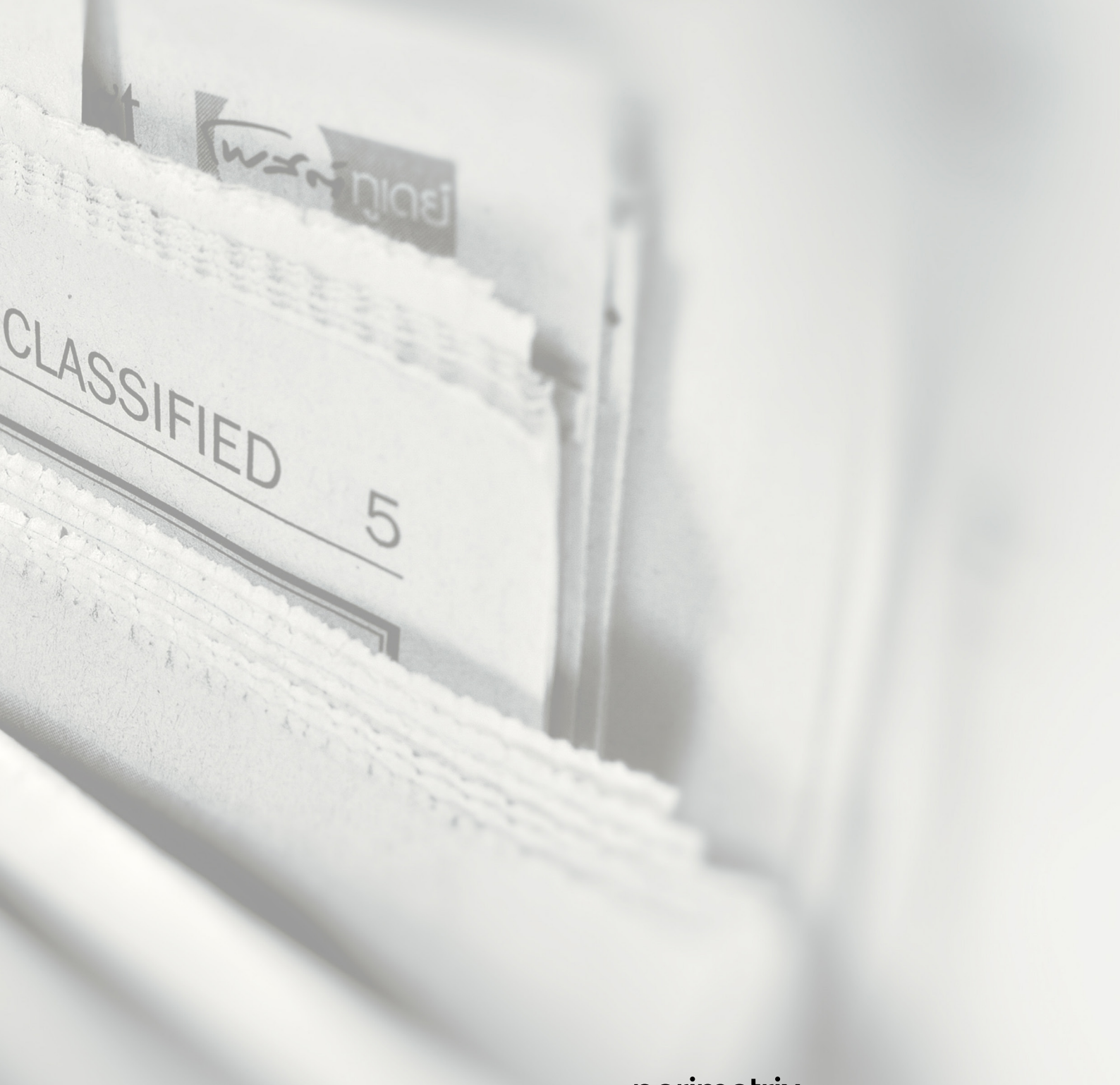
Заключение

Многие современные системы автоматизированного проектирования и электронного документооборота имеют развитые средства разграничения доступа пользователей к хранимому и обрабатываемому в них информационному контенту. Однако в тот момент, когда информация перемещается на рабочий компьютер пользователя, контролировать дальнейшие действия с ней необходимо уже с помощью *специальных защитных средств*, чтобы избежать нежелательных утечек.

Система защиты должна действительно защищать информацию важную и при этом не блокировать информацию, не представляющую значимой ценности, должна не препятствовать «ложными срабатываниями» выполнению легитимных рабочих процессов и не вносить дополнительных бюрократических процедур для пользователей. ■

Все эти возможности дает **PERIMETRIX SAFESPACE**— *система управления классифицированными данными ограниченного доступа.*

ℹ подробная информация о продукте на perimetrix.com



perimetrix

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.