АНДРЕЙ КОГАН,
региональный центр компетенций Периметрикс,
г. Екатеринбург

МАКСИМ ЖАРНИКОВ,
региональный центр компетенций Периметрикс,
г. Екатеринбург

SHUTTERSTOCK.COM/MAXSIM

Вирусная… безопасность

Секреты производства

Право на охрану секретов производства (ноу-хау) закреплено в гл. 75 Гражданского кодекса Российской федерации. Положения этой главы ГК РФ, а также Федеральный закон № 98 служат основой для введения на предприятии режима коммерческой тайны.

Однако законодатель не дает четких инструкций о том, как в реальной практике внедрять режим КТ, из-за чего во многих случаях введение режима на предприятии ограничивается лишь выпуском «Положений о коммерческой тайне» и подписанием с работниками соответствующих пунктов в трудовом договоре.

И это объяснимо. В зоне ответственности службы безопасности предприятия находится огромный спектр разнородных задач – пропускной режим, охрана периметра, физическая безопасность ключевых сотрудников, проверка контрагентов, меры ПДИТР и т. д. Поэтому безопасники просто не в состоянии оперативно отслеживать постоянное возникновение конфиденциальной производственной информации, на ходу определять ее ценность и контролировать все пути ее распространения на предприятии.

А ведь такая информация рождается в процессе производства ежедневно и ежечасно, и ущерб от ее утраты или разглашения может быть весьма критичным для предприятия.

Безусловно, введение на предприятии режима в отношении бумажных конфиденциальных документов частично решает общие задачи режима КТ, но это лишь «вершина айсберга». Во-первых, не всякая конфиденциальная информация производственного характера воплощается в виде печатного документа. Во вторых, до того момента, пока напечатанный бумажный документ не приобретет «защитный» гриф, информация, содержащаяся в его компьютерном первоисточнике, фактически и юридически еще не защищена.

Как быть? Давайте рассмотрим жизненный путь производственного секрета. Такие секреты рождаются в головах разработчиков и конструкторов, руководителей предприятий и подразделений, они также возникают в реальных

ШТАБ-КВАРТИРА PERIMETRIX
РОССИЙСКАЯ ФЕДЕРАЦИЯ,
119607, Москва,
Мичуринский проспект, д. 45
Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92
info@perimetrix.com
www.perimetrix.com

ПРЕДСТАВИТЕЛЬСТВО
PERIMETRIX
НА УРАЛЕ
620142, Екатеринбург,
улица Щорса, д. 7
Телефон: +7 343 278 60 46
Andrey.Kogan@perimetrix.com
Maxim.Zharnikov@perimetrix.com

обстоятельствах производства и эксплуатации производимой продукции.

Производственный секрет – это не личная информация, поэтому обмен такой информацией между сотрудниками предприятия является неотъемлемым элементом производственного процесса. Выбор методов контроля за распространением производственных секретов, безусловно, зависит от того, какими путями этот секрет может передан и в каком виде он может храниться. Человеческий мозг – одно из наиболее распространенных «хранилищ» информации, но его возможности не безграничны и способы отображения информации в нем специфичны. Человек может запомнить суть разговора, идею рисунка, сумму сделки, смысл документа и даже часть его текста, но базу данных, электронную таблицу, многослойный чертеж или сканированную подпись в мозгу сохранить невозможно.

Поэтому для контроля «сведений, составляющих коммерческую тайну» нужно выбирать технические меры, адекватно соответствующие специфике формы, в которой эти сведения представлены. «Простая» информация, которую можно унести в голове, требует от службы безопасности специфических оперативных способов контроля, которые не являются предметом нашего рассмотрения. Передача же более сложной производственной информации требует ее предварительной фиксации на каком-то носителе – на бумаге, в электронном документе, на фото, в виде видео- или аудиозаписи. В современном производстве такая информация, в конечном счете, попадает в информационную систему предприятия, где затем хранится и обрабатывается. Более того, значительная часть такой информации в принципе создается внутри информационной системы, например, дизайнерская документация и конструкторские чертежи.

Изобилие возможностей по обработке и передаче информации в компьютерной среде привело к появлению специфического класса программных продуктов для защиты от утечек, получивших общее название «системы DLP». Такие системы нацелены на перехват информации, передаваемой пользователями по коммуникационным каналам, ее оперативному анализу по заданным шаблонам и принятию решения о допустимости передачи. Наиболее развитые системы DLP позволяют строить модели поведения пользователей, выявлять отклонения и фиксировать инциденты нарушения заданных политик безопасности. Безусловно, поведенческая аналитика может помочь службе безопасности в выявлении реальных и потенциальных нарушителей режима коммерческой тайны. Но на наш взгляд, задачей охраны производственного секрета является предотвращение его утечки, а не ее фиксация. Компьютерные данные, содержащие производственный секрет, для обеспечения их эффективной защиты, должны браться под контроль уже в момент их создания, а не только на выходе, когда конфиденциальной информация пересекает внешнего периметра информационной системы предприятия – при печати, при передаче по электронной почте, размещении в сети Интернет и т. д. Это запоздалая реакция. Режим коммерческой тайны в отношении конфиденциальной производственной информации должен «включаться» уже в тот момент, когда информация фиксируется в виде файла на компьютере пользователя.

Коллективная безответственность и индивидуальная компетентность

Внедрение режима КТ очень часто начинает буксовать на самом старте. Как это происходит?

Приняв решение о необходимости защиты производственных секретов, руководство возлагает на службу безопасности разработку и реализацию мер режима КТ. Попытавшись определить достаточные формальные признаки, по которым информация может быть отнесена к категории коммерческой тайны, служба безопасности быстро приходит к обескураживающему выводу, что любая производственная информация может оказаться коммерческой тайной. Понимая, что на деле это не так, и установка «защитного грифа» на каждый документ просто остановит производственный процесс, служба безопасности умывает руки и апеллирует к ответственности сотрудников, включая требования о соблюдении режима КТ в трудовые соглашения.

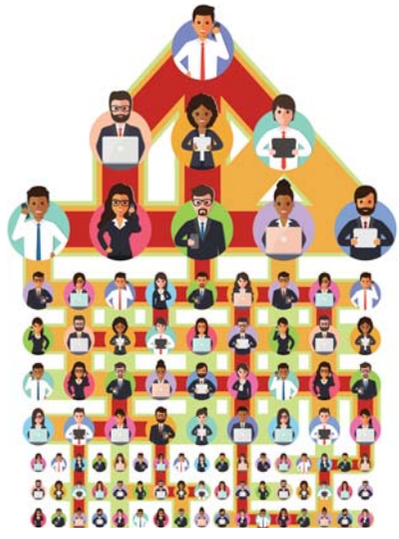
В результате – режим «на бумаге» введен, но уверенности в его соблюдении нет ни у руководства, ни у службы безопасности. Выходом кажется внедрение технических систем отслеживания и анализа действий пользователей в компьютерной среде. Но де-факто это приводит к существенному увеличению объема работы службы безопасности для фиксации и разбора инцидентов и ко всему прочему ухудшает производственный климат в коллективе, а главное – не защищает от возможных утечек. Для руководителя, несущего ответственность за деятельность предприятия в целом, поимка очередного «шпиона» – это не столько показатель эффективности работы службы безопасности, сколько демонстрация неэффективности объявленного режима коммерческой тайны.

Вместе с тем, каждый руководитель прекрасно понимает, что на предприятии есть команда сознательных топ-менеджеров и специалистов, обладающих исчерпывающим пониманием сути и назначения важной производственной информации. Эти люди – «владельцы данных» – способны определить границы «внутреннего периметра» конфиденциальных данных. Именно они являются «опорой режи-

ма», и именно им следует дать в руки инструмент оперативного присвоения конфиденциальной информации «защитного грифа».

Задача службы безопасности становится вполне конкретной – совместно с владельцами данных освоить механизм наложения «защитных грифов», назначить грифы ценной информации и реализовать в отношении нее тот режим безопасного использования и распространения, который продиктован реальными потребностями производственного процесса.

Можно делать только то, что прямо указано и только описанным способом. Все остальное делать «нельзя», и потому должно быть технически невозможно



Запрещено все, кроме того, что разрешено

Режим – это свод жестких предписаний, которые необходимо соблюдать. В отличие от обычных правил поведения, в которых перечисляются запрещенные действия и определяются санкции за их совершение, режим действует по простому и понятному принципу: «Запрещено все. Кроме того, что в явном виде разрешено».

Можно делать только то, что прямо указано и только описанным способом. Все остальное делать «нельзя», и потому должно быть технически невозможно. Именно такой принцип и должен применяться для защиты конфиденциальных сведений, составляющих коммерческую тайну.

При всей кажущейся категоричности, реализация это принципа не только не остановит нормальную производственную деятельность, но и сделает ее более четкой и предсказуемой. Для «правильного» производственного процесса, в котором функционируют защищаемые данные, нужно описать минимально необходимый для нормальной работы периметр их распространения – допустимые места хранения, допустимые программы для обработки, допустимые принтеры для печати, список допущенных сотрудников. В процессе реальной работы изначально заданный периметр может расширяться. Но всякий раз это расширение будет являться сознательным действием, отражающим уточнение необходимой цепочки производственного процесса, и конфиденциальные данные не покинут периметр, пока такая возможность не будет определена в параметрах режима в явном виде.

«Заражение» безопасностью

Широко распространено опасение, что внедрение режима остановит работу предприятия. Чтобы этого не произошло, необходимо реализовать баланс между жесткой защитой производственных секретов и гибким производственным процессом. Поэтому, в идеале, периметр безопасности должен расширяться постепенно, по мере уточнения производственной цепочки, в которой циркулирует конфиденциальная информация.

Начиная свое движение внутри организации, маркированная «защитным грифом» информация заново верифицирует привычную траекторию ее распространения, требуя от владельца данных принять осознанное решение о допуске к ней новых сотрудников, о разрешении новых мест хранения и способов обработки. Расширение круга «секретоносителей» происходит не по формальному признаку их принадлежности к той или иной структурной единице предприятия, а в результате их «соприкосновения» с конфиденциальной информацией, продиктованного реальной производственной необходимостью.

Второй путь «естественного» расширения периметра безопасности основан на следующем принципе: отнесение документа к категории КТ означает, что все созданные на его основе документы также следует по умолчанию относить к КТ, поскольку они могут содержать защищаемый контент. И только осознанное решение владельца данных или службы безопасности может избавить их от «защитного грифа». Такой подход избавляет службы безопасности постоянного принятия однотипных решений в отношении вновь создаваемых документов.

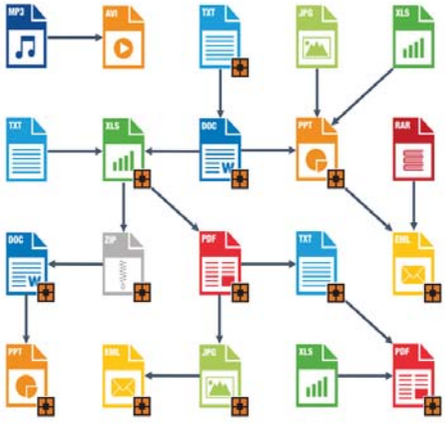
Так режим распространяется по предприятию, словно вирус – от владельцев данных к другим сотрудникам, от одного защищенного документа – ко всем его производным. Безопасный периметр режима КТ постепенно охватит все производственные цепочки, в которых используется конфиденциальная информация, не затронув при этом остальную жизнь предприятия.

Техническая реализация режима коммерческой тайны

Защитный программный комплекс «Периметрикс», разработанный одноименной российской компанией, в точности реализует описанный выше подход. Механизм работы комплекса основан на присвоении информационным объектам классификационных меток.

Классификационная метка может быть присвоена компьютерной информации различными способами.

Первый – это присвоение метки вручную, осознанным действием от-



ветственного исполнителя, формирующего конфиденциальный документ.

Второй способ – автоматическое формирование метки на основе заранее определенных правил. Например, все чертежи, создаваемые конструкторами в программе AutoCAD или КОМПАС, могут получать метку уже в момент их сохранения в файл, и все дальнейшие действия с ними – вывод на печать, копирование и т. д. будут выполняться в точном соответствии с установленными требованиями режима.

Третий способ – это наследование метки. Перенос информации из «помеченного» файла в другой – путем ли создания копии файла, конвертации его в другой формат, или даже копированием содержимого через буфер обмена – приведет к тому, что вновь создаваемый объект получит ту же классификационную метку, которая была у исходного. Любая копия конфиденциального документа или производный документ по-прежнему останется конфиденциальным – в отношении его будут действовать те же правила режима.

«Выпуск» конфиденциальной информации за пределы защищаемого периметра регламентируется правилами режима. Например, вывод на печать может быть разрешен только на принтер, где организован учет бумажных экземпляров. Пересылка классифицированной информации по электронной почте или копирование на мобильные носители может быть разрешена только в зашифрованном виде. Поэтому открыть такое письмо или файл сможет только доверенный пользователь, на компьютере которого уже установлен комплекс «Периметрикс» и который обладает достаточными правами для работы с классифицированной информацией.

Рассмотрим теперь сценарий «естественной» реализации режима коммерческой тайны на предприятии. Высшее руководство компании, службы режима и экономической безопасности, включенные в первоначальный «периметр безопасности», в процессе ежедневной работы создают документы, содержание которых составляет коммерческую тайну. При работе под контролем комплекса «Периметрикс» эти документы приобретают соответствующие классификационные метки. Если производственный процесс потребует ознакомления с этими документами некоторых нижестоящих сотрудников, владельцы данных могут принять решение о расширении круга допущенных к коммерческой тайне и установки на их компьютерах необходимого защитного ПО.

Конфиденциальные документы, помеченные владельцами данных, могут быть использованы в качестве образцов при инвентаризации уже имеющихся информационных активов. Таким способом служба безопасности сможет обнаружить на компьютерах пользователей и оперативно защитить ранее созданные конфиденциальные данные.

Механизм наследования меток и применение «помеченных» шаблонов помогает пользователям оставаться в рамках режима при создании новых регулярных документов, содержащих КТ.

Более того, в отношении заведомо ценных данных (например, проектно-конструкторской документации или персональных данных) может быть принято решение об их тотальной автоматической маркировке в момент создания.

Заключение

Подытожим основные преимущества такой реализации режима коммерческой тайны на предприятии:

- Режим КТ в отношении компьютерной информации строится не по формальным признакам, а на основе реальных знаний о ценности сведений, относимых к КТ.
- Инициаторами отнесения информации к КТ являются компетентные владельцы данных, а не обособленная служба безопасности.
- Построение режима коммерческой тайны может начинаться поэтапно и независимо в разных подразделениях, работающих с разными типами конфиденциальной информации (производственные данные, коммерческая информация, персональные данные и т. п.).
- Реализуется принцип минимальных полномочий – к работе с конфиденциальной информацией допускаются только те пользователи, которым это реально необходимо.
- Принятие решение об отнесении информации к категории «защищаемой» принимается оперативно, в момент ее создания в компьютерной среде. Это может выполняться системой автоматически, на основе предустановленных правил, а также вручную – ответственными сотрудниками.
- В отношении классифицированной информации реализуется основной принцип режима – «Запрещено все, кроме того, что в явном виде разрешено». Такой подход обеспечивает сохранность конфиденциальных данных и не препятствует нормальному производственному процессу.
- Вывод информации за пределы безопасного периметра или снятие классификационных меток производится только по правилам режима и под контролем службы безопасности.

Добавим, что наш комплекс защищает проектную и конструкторскую документацию на предприятиях машиностроения, персональные данные в государственных структурах, обеспечивает режим коммерческой тайны на предприятиях энергетики и нефтегазового сектора и т. д. ●