

## ■ Защита корпоративной информации от инсайда

■ Михаил Калинин, генеральный директор компании StarForce Technologies

**В**опрос защиты корпоративной информации от инсайда можно разделить на две составляющие: контроль над использованием в компании стороннего ПО и защита электронной документации, вращающейся как внутри организации, так и за ее пределами. Если говорить о кризисе, то, на мой взгляд, по сравнению с более благополучными годами мало что изменилось. По-прежнему существует риск хищения информации и вынос ее за стены предприятия. Пожалуй, в кризис количество работников, недовольных своей судьбой, возросло, а значит, возросла и вероятность ответных действий со стороны недовольного сотрудника. Читая различные высказывания в отечественной блогосфере, я неоднократно наткнулся на примеры мести со стороны работников, которых сократили или которым попросту снизили зарплату.

Если говорить о контроле над использованием ПО, то представляется очень важным строго разграничить доступ сотрудников к определенным ресурсам предприятия. Условно говоря, сотрудники отдела технической поддержки не должны иметь доступ к финансовым документам, а сотрудники бухгалтерии — к информации, описывающей инновационные разработки компании. Кроме того, нужно контролировать количество и качество ПО, устанавливаемого на компьютерах работников. В этой связи необходимо принимать меры по ограничению прав пользователей на своих машинах.



Кроме того, важно ограничить использование внутрикорпоративного ПО таким образом, чтобы не все пользователи могли свободно запускать ту или иную программу, позволяющую им, например, получить доступ к базе данных сотрудников или клиентов предприятия. Существующие на рынке решения позволяют ограничивать не только количество одновременно запущенных копий программы в корпоративной сети, но и время их работы,

их функционал. Ограничение вывода на печать, ограничение доступа к USB-шине или оптическим дисководом, установленным на компьютере, позволят не лишать работника таких важных компонентов современного компьютера, как USB-устройства или приводы компакт-дисков. В то же время надлежащая защита внутрикорпоративного ПО не позволит воспользоваться этими устройствами, когда это может вызвать пагубные последствия. В этом случае работник не сможет переписать важные данные на флешку или на диск и вынести с предприятия,

не сможет скопировать их и отправить по электронной почте или просто распечатать на принтере. Что касается защиты электронной документации, то это, пожалуй, самый главный аспект. Потому что в рамках предприятия всегда существуют лица, которые обладают достаточно высоким уровнем доступа, чтобы свободно вносить и выносить с предприятия носители с информацией. Попадание последних к злоумышленникам может повлечь очень серьезные потери для компании. А если ваш бизнес связан с производством интеллектуальной собственности и зависит от продаваемых тиражей, степень угрозы возрастает в геометрической прогрессии. К таким конфиденциальным да нным относятся и прайс-листы, информация о сроках разработки и запуска продук-

изменениям. Происходит это следующим образом: после защиты документы становятся неотделимы от программ их просмотра, которые, в свою очередь, привязываются к компьютеру. Тогда документ можно открыть только на определенном компьютере (где установлена эта программа), имея при этом активационный ключ. То есть человек, отвечающий за безопасность данных в документе, защищает документ с помощью веб-сервиса, высылает его адресату вместе с программой просмотра и сообщает получателю серийный номер, с помощью которого тот сможет провести активацию документа. После этого документ можно будет просмотреть только на этом компьютере — и ни на каком другом. При защите корпоративного информационного пространства необходимо использовать

**Необходимо защищать каждый конкретный документ, содержащий в себе конфиденциальную информацию, перед его отправкой за пределы компании.**

тов, о маркетинговых кампаниях и результатах продаж и многое другое. Следовательно, все эти данные нуждаются в защите. В основном такая информация хранится в виде электронных документов в корпоративной сети. Когда документы отправляются за пределы компании, хочется быть уверенными в том, что они не уйдут «в третьи руки». Поэтому необходимо защищать каждый конкретный документ, содержащий в себе конфиденциальную информацию. В большинстве случаев это возможно, если документ уже сформирован и не должен подвергаться

целый комплекс мер, в том числе антивирусные продукты, решения на базе поведенческого анализа, контроль доступа и использования программного обеспечения, защиту электронных документов и многое другое. На обеспечение сохранности информации должны быть нацелены усилия всех подразделений компании, будь то отдел ИТ-безопасности или отделы маркетинга и HR. ◀