

как правило, не вызывают особого энтузиазма у персонала. Неприятно осознавать, что за вами ведется постоянное скрытое наблюдение, каждый шаг контролируется, а все операции на персональном компьютере протоколируются. Мониторинг действий пользователей при помощи особого программного обеспечения является мощным оружием в борьбе с инсайдерами, мошенниками и недобросовестными сотрудниками, однако оно требует крайне осторожного обращения. Использование методов защиты должно учитывать и определенные этические моменты, дабы не настроить против компании и ее руководства лояльных и законопослушных работников.

По мнению специалистов, политика безопасности предприятия должна четко определять, что вся информация, хранимая, обрабатываемая и передаваемая по каналам связи в корпоративной сети является ее собственностью. Это необходимо довести до ведома каждого работника, например, посредством заключения соответствующего договора о неразглашении или расписки. Сотрудников — пользователей информационных систем компании — нужно предупредить о том, что все системы находятся под

наблюдением, и в случае совершения несанкционированных действий к ним будут применены меры дисциплинарного, материального или другого воздействия. Должен быть запрещен несанкционированный доступ, раскрытие, дублирование, изменение, удаление и ненадлежащее использование данных и разрешено применение служебной информации только в производственных целях. Границы допустимого использования определяются руководством компании в соответствующих инструкциях (положениях).

При этом важно формировать у сотрудников понимание необходимости очень бережного отношения к коммерческой тайне. Необязательно рассказывать о том, каким образом и насколько подробно осуществляется мониторинг их действий. Достаточно того, чтобы они осознали всю серьезность угрозы утечки информации и то, что компания обязана принимать меры по ее защите, чтобы выжить в конкурентной борьбе. Вместе с тем, руководство организации должно запрещать службе безопасности изучать личную и служебную переписку сотрудников в отсутствие признаков угрозы и вне рамок проведения служебных расследований. **Д**



**Артем Неповека,**  
специалист по технической защите информации в компьютерных системах компании «Арт-мастер»

### О ситуации с инсайдерами

Инсайдер — это лицо, имеющее доступ к конфиденциальной информации компании в силу своего служебного положения либо родственных связей. Это может быть человек, специально посланный в организацию, который устраивается на работу как обычный сотрудник и получает доступ к секретным данным, используя как прикрытие исполнение своих служебных обязанностей. Инсайдером может считаться служащий, согласившийся передавать закрытую информацию компании третьей стороне (не имеющей права доступа к таким сведениям). В любом случае, инсайдером сотрудник становится именно в момент передачи данных.

### О мерах противостояния

Следует также отметить то, что не отдельные мероприятия, а только комплекс организационных и инженерно-технических мер может эф-

фективно противостоять инсайдерам. К организационным мероприятиям необходимо отнести и периодическое тестирование сотрудников на соблюдение ими правил безопасной работы, и проведение разъяснительных бесед. Именно разъяснительных, а не простой диктовки правил, в большинстве из которых содержится запрет какого-либо действия. При этом обязательно необходимо учитывать психологический фактор, потому что, как известно, запретный плод сладок.

Теперь представьте, сколько подобных «плодов» получает работник во время проведения начального или периодического инструктажа на предприятии. В случае если он чем-то не удовлетворен, такое напутствие может послужить прямым руководством к действию. Поэтому нужно объяснить, что несоблюдение того или иного правила приведет к последствиям, которые отразятся на всей компании и непосредственно на каждом сотруднике.

Кроме того, необходимо: проинструктировать сотрудников, как вести себя, если к ним обратятся с предложением предоставить конфи-

денциальную информацию о предприятии; объяснить, что, продав такие сведения, они получат лишь одноразовое вознаграждение, но потеряют работу и, возможно, даже не смогут больше устроиться в данной сфере. Такие меры позволяют всему коллективу компании участвовать в процессе защиты данных. Если какой-либо работник станет причиной информационного мошенничества, остальные могут обнаружить это и предупредить утечку самостоятельно либо обратиться в службу безопасности.

### О направлениях защиты

Основные силы по обеспечению защиты следует направить на электронные каналы утечки данных, но не стоит также сбрасывать со счетов и акустический. Самый простой из них — подслушивание разговоров. Если в компании часто проводятся секретные переговоры, в которых фигурирует секретная информация, необходимо выделить для этого отдельное помещение, используя специальные технические средства и организационные меры, позволяющие исключить возможность подслушивания.

## СЛОВО ЭКСПЕРТА