# Обезвредить врага внутреннего

## Как банку защититься от инсайдеров

**Понятие информационной безопасности традиционно связывают с защитой от внешних угроз — вирусов, хакерских атак, шпионских программ, спама и т.д. Однако в последнее время IT-специалисты все чаще говорят об актуальности внутренних угроз — об умышленных и неумышленных действиях собственных сотрудников**

*Текст*
**ДМИТРИЙ СЛОБОДЕНЮК,**
КОММЕРЧЕСКИЙ ДИРЕКТОР КОМПАНИИ ARINTEG

Согласно опросу, проведенному компанией BalaBit среди 300 респондентов, 84 % рисков нарушения информационной безопасности обусловлены человеческим фактором. Сюда можно отнести случайные и намеренные ошибки персонала, активность внутренних и внешних злоумышленников. В то же время всего 16% угроз респонденты отнесли к проблемам, связанным с IT-инфраструктурой компании.

Тот же опрос показал, что несмотря на значительный перевес в оценке различных рисков бюджеты на обеспечение информационной безопасности все же распределяются в компаниях более или менее сбалансированно: 55% финансирования отправляются на защиту от рисков, связанных с человеческим фактором, и 45% — на инфраструктурные угрозы.

Более того, когда респонденты столкнулись с вопросом о том, какой фактор приводит к максимальным материальным убыткам, 51% указали именно на человеческий фактор. В то время как только 13% сказали, что при планировании бюджета, прежде всего, распределяют средства на решение именно этой проблемы.

Если компании намерены тратить свой бюджет ответственно и эффективно, то сейчас самое время покончить с существующими заблуждениями: продвинутый мониторинг может стать хорошим оружием против рисков, связанных с человеческим фактором, вне зависимости от того, является ли источник угрозы внешним или внутренним, случайным или намеренным. Современные решения позволяют не только контролировать действия пользователей, но и обнаруживать инциденты ИБ, находить взаимосвязи между разрозненными событиями и выявлять недобросовестные намерения пользователей.

Особо хотелось бы отметить системы контроля действий, пожалуй, самых осведомленных пользователей корпоративной сети — системных администраторов. Для полноценного обеспечения информационной безопасности необходимо понимать, какие права они имеют и для чего они их используют. Немаловажную роль играют такие системы для контроля сторонних организаций, осуществляющих обслуживание компонентов IT-инфраструктуры компании на условиях аутсорсинга. Иначе, передавая подрядчикам на обслуживание критически важные для бизнеса объекты без должного контроля над их действиями, повышаются риски противоправных действий, приводящих к негативным для компании последствиям.

Такие риски могут быть значительно снижены благодаря активному обнаружению и блокированию подозрительной активности пользователей, в первую очередь привилегированных пользователей, так как они, как правило, имеют почти неограниченные права по доступу к информационным активам компании и становятся главной мишенью хакеров. Система мониторинга действий таких пользователей способна контролировать сеансы работы собственных и сторонних администраторов, своевременно выявлять аномальную активность, позволяет оперативно ее заблокировать и провести полноценное расследование инцидента. Таким образом, повышается уровень информационной безопасности компании, а также выполняются регуляторные требования по ИБ, например, PCI DSS. Б.О