

Как защитить коммерческую тайну от инсайдеров?

Обеспечение конфиденциальности информации о клиентах, финансовых операциях, планируемых маркетинговых акциях — важнейший принцип развития современной компании. Сохранять конфиденциальность — обязанность каждого сотрудника.

Кто мешает выполнять эту обязанность? Ведь есть закон, гласящий о наказании за разглашение коммерческой тайны. Работают квалифицированные сотрудники безопасности, которые обеспечивают сохранность информационного ресурса. Все это так. Но распространенной ошибкой является уверенность, что главный источник информационных угроз находится за пределами компании.

Реальным источником опасности для компании являются **инсайдеры**. Инсайдеры — это сотрудники компании, имеющие доступ к информации, составляющей коммерческую тайну. Они становятся причиной утечки информации в результате стечения разных обстоятельств, например:

- ◆ Увольнение сотрудника (особенно в условиях конфликта). Вероятное последствие — изъятие важной для компании информации с целью отомстить работодателю.

- ◆ «Охота за головой» сотрудника компании. Вероятное последствие — изъятие и передача новому работодателю ценной информации с целью карьерного продвижения или получения выгодного социального пакета.

- ◆ Симпатия между сотрудниками компании. Вероятное последствие — обмен конфиденциальными данными во время совместного досуга и последующее нецелевое использование услышанного одним из сотрудников и т.д.

Вы уверены, что конфиденциальная информация не станет жертвой одного из этих вариантов поведения сотрудников вашей компании? Как можно обезопасить информационный ресурс от человеческого фактора? Ответ есть. Это внедрение **Системы информационной безопасности (СИБ)**.

СИБ — это комплекс мер по обеспечению информационной безопасности компании. В отношении инсайдеров СИБ является уникальным защитным инструментом, который не блокирует злой умысел или халатность (что в принципе невозможно), а предотвращает их возникновение и воплощение в жизнь.

Одним из важных этапов внедрения СИБ является выбор организации-исполнителя (далее — Исполнитель), которая будет внедрять в компании СИБ. Это очень важно, так как Исполнитель, проектирующий СИБ компании, обя-

зательно должен соответствовать таким требованиям:

- ◆ наличие международных сертификатов, подтверждающих профессионализм сотрудников Исполнителя;

- ◆ наличие сертифицированной системы управления качеством (ISQ/IEC9001:2000), обеспечивающей соответствие конечного продукта (СИБ) мировым требованиям;

- ◆ наличие сертифицированной системы управления информационной безопасностью (ISO/IEC 27001:2005), которая дает уверенность в том, что Исполнитель имеет не только опыт внедрения систем во внешних организациях, но и эффективно поддерживает работоспособность своей СИБ;

- ◆ наличие лицензий государственного образца, дающих Исполнителю право выполнять работы по технической и криптографической защите информации.

Компания «Арт-мастер» полностью отвечает всем вышеперечисленным требованиям. СИБ, спроектированная и внедренная компанией «Арт-мастер», — надежный щит от внешних и внутренних посягательств на вашу конфиденциальную информацию. ☒

Компания «Арт-мастер»

предлагает следующие услуги в сфере защиты информации:

- ▶ построение комплексных систем защиты информации;
- ▶ проведение государственных экспертиз в сфере технической защиты информации;
- ▶ построение систем менеджмента информационной безопасности в соответствии с требованиями стандарта ISO 27001:2005;
- ▶ проведение аудитов информационной безопасности;
- ▶ предоставление услуг электронной цифровой подписи.



**Центральный офис
ООО «Арт-мастер»**

ул. Сурикова, 3 (лит. А), Киев,
03035, Украина
тел. +380 44 248-97-91, 248-98-27
факс. +380 44 248-98-14
e-mail: post@am-soft.ua
http://www.am-soft.ua

Symantec отмечает охоту хакеров за конфиденциальными данными

В очередном, XIII, томе Отчета об угрозах Интернет-безопасности (Internet Security Threat Report), который представила корпорация Symantec, сделан вывод, что роль главного проводника вредоносной деятельности перешла от корпоративных сетей к Всемирной паутине и что пользователи подвергаются все большему риску, просто посещая веб-сайты. Symantec обращает внимание на то, что хакеры особенно облюбовали сайты, пользующиеся доверием, такие как сайты социумных сетей.

За последние шесть месяцев 2007 года в Интернете было зарегистрировано 11 253

отдельных веб-сайта, уязвимых к атакам методом межсайтового скриптинга. И за этот период администраторами были исправлены всего 473 (около 4%) из них. Кроме того, за последние шесть месяцев 2007 года Symantec зарегистрировала 87 963 фишинговых хоста — компьютера, на которых могут располагаться один или несколько фишинговых сайтов. Это на 167% больше, чем в первом полугодии 2007 года. 80% целенаправленных фишинговых атак в течение отчетного периода относились к финансовому сектору. ☒