

ISO / IEC 27001:2005 — рыночное преимущество банка

С одной стороны, разрабатываются и успешно внедряются решения, которые помогают человеку — значительно повышают коэффициент полезного действия умственного и ручного труда, оптимизируют производственные процессы, быстро обрабатывают большие массивы информации. С другой стороны, создаются и используются информационные технологии, которые могут нанести человеку ощутимый вред — провоцируют аварийные ситуации на объектах транспортных систем и сбои в системах тепло- и электроснабжения, замедляют производственные процессы, приводят к утечке информации, находящейся под грифом разного уровня секретности. Движение по этим векторам, которое проявляется в развитии «полезных» и «вредных» для человека информационных технологий, происходит фактически параллельно. Сегодня в потенциальной опасности находятся информационные ресурсы большинства организаций, работающих в таких сферах, как экономика (производственные предприятия, сектор финансовых услуг, торговые сети и т.д.), государственное регулирование (органы законодательной, исполнительной и судебной власти, органы местного самоуправления), социально-гуманитарное управление (медицинские, учебные, культурные учреждения), международные отношения (представительства международных организаций и миссий, посольства и консульства, экспортно-импортные фискальные органы и др.). Но наибольшая опасность грозит информационным инфраструктурам банковских учреждений, представляющим собой территорию оборота больших объемов финансовых ресурсов — предмета такого же

Стремительное развитие информационных технологий как современное явление и процесс, прогрессирующий во всех сферах человеческой жизнедеятельности — от домашнего быта до освоения космоса, имеет две стороны медали.

большого интереса различных преступных групп.

В таких условиях приоритетной задачей для украинских ИТ-компаний становится разработка и внедрение комплексных систем информационной безопасности, которые способны не столько отреагировать на негативное влияние на информацию постфактум, сколько предотвратить такое влияние. Разрозненные мероприятия по защите информационного ресурса или установка отдельного защитного программного обеспечения не могут эффективно защитить информацию от всего арсенала информационных угроз. Вынужденное обращение к внешним специалистам в аварийных ситуациях исключает правильный выбор адекватного набора услуг, а также ИТ-компания-исполнителя, которая должна иметь подтвержденный опыт в сфере информационной защиты. Иными словами, речь идет о построении и создании системы менеджмента информационной безопасности (СМИБ), которая должна соответствовать требованиям международных стандартов. В области информационной безопасности официальным и всемирно признанным показателем качества является международный стандарт ISO/IEC 27001:2005 «Информационные технологии — Методы защиты — Системы менеджмента информационной безопасности — Требования», разработанный Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) на основе британского стандарта BS 7799-2:2002.

По данным ISMS International User Group, сегодня в мире выдано более 4000 сертификатов.

Компания «Арт-мастер», работающая на украинском рынке информационных технологий уже более восьми лет, стремится предлагать те решения, которые приносят максимальную пользу обществу в целом и каждому конкретному клиенту в частности.

Деятельность «Арт-мастер» в области защиты информации представлена широким спектром услуг: аудит информационной безопасности, построение и внедрение систем информационной безопасности (СИБ) и комплексных систем защиты информации (КСЗИ), подготовка предприятия к сертификации системы менеджмента информационной безопасности на соответствие с требованиями международного стандарта ISO/IEC 27001:2005. В 2006 году компания получила сертификат соответствия системы менеджмента информационной безопасности требованиям этого международного стандарта, а в 2007 году успешно прошла надзорный аудит, подтверждающий соответствие СМИБ компании требованиям международного стандарта ISO/IEC 27001:2005. Этот факт свидетельствует о положительной международной оценке практического опыта компании «Арт-мастер» по внедрению у себя СМИБ и высокому качеству услуг компании в данной сфере.

Внедрение в инфраструктуру банка СМИБ в соответствии с требованиями международного стандарта ISO/IEC 27001:2005 позволит руководству нагляд-

но продемонстрировать деловым партнерам, инвесторам, клиентам и международным наблюдательным органам, что в банке налажена эффективная система информационной безопасности. Это означает, что кредит доверия к банку будет расти, так как гарантированная сохранность банковской тайны является огромным рыночным преимуществом в банковском сегменте. Сотрудники департамента защиты информации компании «Арт-мастер» окажут профессиональную техническую и консультационную поддержку ИТ-подразделению банка на всех этапах разработки СМИБ:

- определение области применения СМИБ;
- разработка Политики информационной безопасности;
- разработка подходов к оценке рисков;
- идентификация рисков;
- анализ и оценка рисков;
- принятие решения по обработке рисков (применить к риску соответствующие средства управления/принять риск в соответствии с разработанными критериями принятия рисков/избежать риска/передать риск другой стороне);
- выбор средств управления, которые можно применить для уменьшения рисков;
- получение согласия руководства по остаточным рискам;
- подготовка Положения о применимости — одного из обязательных документов СМИБ.

■ **Сергей Мальчиков,**

и. о. руководителя отдела по технической и криптографической защите информации
ООО «Арт-мастер»