

**Александр Пачев, директор компании «Арт-мастер»**  
**«Философия "Арт-мастер" — профессиональные ИТ-решения»**



**ГИС-направление.** Мы являемся партнером компании Intergraph, которая более 35 лет работает на рынке САД- и ГИС-систем. Продукты и решения Intergraph используются в более чем 60 странах мира. Основные наши усилия направлены на использование технологии этой компании в своих разработках, а не на продажу ее «коробочных» продуктов.

Особенностью ГИС-решений является то, что, помимо пользовательских данных, в системе должны быть геопространственные данные, на которые эти пользовательские данные должны быть наложены. Пользовательские данные являются продуктом деятельности клиента, в то время как геопространственные должны поставляться клиенту вместе с ГИС-решением. Мы столкнулись с проблемой отсутствия полных и актуальных геопространственных данных по территории Украины. На одном из мероприятий, мы познакомилась с технологией сбора геопространственных данных, применяемой в США, и решили перенести ее на территорию Украины: приобрели специальное оборудование, разработали специальное программное обеспечение, технологию и методику съемки, позволяющие собирать геопространственные данные в режиме реального времени в процессе движения автомобиля. С помощью технологии «Фазтон» мы собрали и актуализировали информацию по 16 городам областного значения и к середине 2008 года планируем создать

полную базу данных по всем областным центрам Украины. Она будет включать данные о дорожной сети, перечень улиц и наименования объектов, основные объекты картографии, топонимы и видеолог (кол-

лекция изображений объектов, расположенных вдоль элементов дорожной сети, угол съемки 180 градусов).

Разработанная «Арт-мастер» система мониторинга и управления транспортными средствами Fleet Management позволяет отслеживать местоположение транспортных средств в реальном времени, контролировать их перемещение и остановки. Система имеет мощную аналитическую функциональность: построение оптимальных маршрутов, контроль выполнения заданий, контроль пересечения заданных зон, формирование графических и текстовых отчетов и др. Ее использование позволяет вывести на качественно новый уровень решение важных задач эксплуатации транспорта: мониторинг транспортных средств, логистику, борьбу со злоупотреблениями, повышение производительности труда и дисциплины персонала, сокращение расходов ГСМ, повышение качества обслуживания клиентов.

**Защита информации.** Департамент защиты информации «Арт-мастер» сегодня ведет работу в трех направлениях:

- построение комплексных систем защиты информации (КСЗИ), систем информационной безопасности (СИБ), а также предоставление услуг по проведению аудита информационной безопасности (АИБ);

- проведением государственных экспертиз КСЗИ (в 2007 году мы были внесены в Реестр организаторов государственной экспертизы в сфере технической защиты информации).

- в состав департамента защиты информации входит аккредитованный центр сертификации ключей MASTERKEY, который предоставляет полный спектр услуг электронной цифровой подписи (ЭЦП). Благодаря наличию филиальной сети компании «Арт-мастер» клиенты могут приобрести ЭЦП в любом из 24 областных центров Украины, в г. Симферополе и г. Киеве.

**Учебный центр.** В январе 2008 года наш учебный центр стал авторизованным учебным центром Prometric. Теперь в нем можно пройти авторизованное тестирование и получить международный сертификат Microsoft, Oracle, Novell, Sun Microsystems, Citrix, Hewlett-Packard, Linux Professional Institute, IBM, Intel, CompTIA, Adobe, 3Com, EMC, Dell и других вендоров. Авторизованное тестирование — это четко отработанная процедура сдачи экзаменов различных вендоров в одном из тестовых центров, расположенных по всему миру. Услуги тестирования и сертификации являются логичным завершением цикла обучения.

♦ *ComputerWorld/Украина № 13 '2008*

**ISO/IEC 27001:2005 — рыночное преимущество банка**

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.

Деятельность компании «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 требованиям международного стандарта ISO/IEC 27001:2005 «Информационные технологии — Методы защиты — Системы менеджмента информационной безопасности — Требования».

Внедрение СМИБ в соответствии с требованиями международного стандарта ISO/IEC 27001:2005 приведет к тому, 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 (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.

♦ *Директор информационной службы № 3 '2008*

**Правовые и организационные основы комплексных систем защиты информации**

Комплексные системы защиты информации (КСЗИ) объединяют организационные и инженерно-технические мероприятия, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Режимно-секретный орган (РСО) — это отдел или подразделение, в котором создается, обрабатывается и хранится информация с ограниченным доступом: конфиденциальная информация, принадлежащая государству, и информация, содержащая государственную тайну. В большинстве случаев такая информация обрабатывается с использованием АС класса 1. Основными потребителями КСЗИ РСО являются органы государственной власти, а также предприятия, работа которых связана с информацией, содержащей государственную тайну.

В АС класса 2 и класса 3 обрабатывается конфиденциальная или открытая информация, которая принадлежит государству и к которой выдвигаются требования по обеспечению целостности и доступности. Потребителями КСЗИ АС класса 2 и класса 3 являются органы государственной власти, а также предприятия, деятельность которых связана с обработкой конфиденциальной информации, принадлежащей государству.

Системы информационной безопасности (СИБ) в основном предназначены для защиты информации в АС класса 2 и класса 3. СИБ можно рекомендовать коммерческим организациям, которые заботятся о сохранности своей коммерческой информации или собираются принимать меры по обеспечению безопасности своих информационных активов.

Сравнительный анализ всех перечисленных систем представлен в таблице.

♦ *Директор информационной службы № 2 '2008*

Особенности	КСЗИ РСО	КСЗИ АС класса 2 (3)	СИБ
Потребители услуг	Органы государственной власти, коммерческие организации	Органы государственной власти, коммерческие организации	Коммерческие организации
Обрабатываемая информация	Конфиденциальная информация, которая принадлежит государству, или информация, которая содержит государственную тайну	Конфиденциальная информация, которая принадлежит государству (физическому лицу), или открытая информация, которая принадлежит государству	Критическая информация организации (персональная, финансовая, договорная информация, информация о заказчике)
Субъекты	Заказчик Исполнитель Контролирующий орган	Заказчик Исполнитель Контролирующий орган	Заказчик Исполнитель
Наличие лицензии на проведение работ по построению	Лицензия на проведение работ по технической защите информации	Лицензия на проведение работ по технической защите информации	Не требуется
Проведение государственной экспертизы	Обязательно	Обязательно	Не требуется
Технические средства защиты информации	Только сертифицированные средства защиты информации	Только сертифицированные средства защиты информации	Любые средства защиты информации
Выполнение требований нормативной базы	Обязательно	Обязательно	Не требуется

**Аудит информационной безопасности**

В настоящее время все без исключения организации используют информационные системы для передачи, хранения и обработки информации, и очень велика вероятность утечки конфиденциальных данных. Кража важной информации, халатность сотрудников, саботаж, атаки хакеров могут нанести существенный удар как по финансам, так и по имиджу любой компании. Предотвратить риски поможет грамотно проведенный аудит информационной безопасности.

**Необходимый элемент безопасности**

Наиболее важный вопрос информационной безопасности — «Как именно информация утекает?». Ответ на него сможет дать аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с критериями информационной безопасности.

Важно понимать, что это не единоразовое мероприятие, а регулярный процесс, который должен проводиться с заданной периодичностью. Многие руководители организаций заблуждаются, думая, что, проведя один раз аудит информационной безопасности, выявив каналы утечки информации и приняв соответствующие меры по нейтрализации этих каналов, они полностью обеспечат защиту корпоративной информационной системы. Это не так, ведь современные технологии не стоят на месте, а развиваются очень быстро.

**Каналы утечки информации**

По результатам исследования компании InfoWatch, наибольшее количество утечек (50%) произошло через ноутбуки, КПК, USB-флэшки, CD- и DVD-диски и другие устройства. Следующий канал — Интернет (12%). Еще 5% случаев нарушения информационной безопасности произошло из-за неправильной утилизации или потери резервных носителей. По 3% пришлось на электронные

послания и факсы, а также почту. 17% случаев нарушения внутренней информационной безопасности произошли по другим каналам. В 10% случаев так и не удалось выяснить, каким образом была произведена кража.

**Особенности аудита**

Грамотно проведенный аудит информационной безопасности поможет снизить риски организации и увеличить уверенность в собственной системе безопасности. Руководителю ИТ-отдела необходимо знать, что аудит информационной безопасности даст ему перечень каналов утечки информации в организации, рекомендации по нейтрализации этих каналов, перечень угроз и оценку рисков по каждой угрозе, а также поможет сформировать необходимый комплекс защитных мероприятий и разработать план их реализации.

«Арт-мастер» предоставляет услуги по проведению аудитов информационной безопасности двух видов.

Результатом **экспертного** аудита является общая оценка защищенности корпоративной информационной системы организации, которая основана на анализе рисков и перечне обнаруженных уязвимостей. По итогам аудита формируется отчет и разрабатываются рекомендации для нейтрализации выявленных уязвимостей.

В результате аудита **на соответствие международному стандарту ISO/IEC 27001:2005** руководитель организации получает описание области действия системы менеджмента информационной безопасности, реестр важных активов, методику оценки рисков, отчет по оценке рисков, критерии принятия рисков, а также список политик, руководств, процедур и инструкций, необходимых для функционирования системы менеджмента информационной безопасности.

♦ *Директор информационной службы № 2 '2008*

Арт-мастер  
(044) 248-97-91  
www.am-soft.ua