

# СТРАТЕГИИ И МНЕНИЯ

## Размышления об информационной безопасности

**В** УКРАИНЕ В ПРОМЫШЛЕННОМ И торговом секторе экономики состояние систем обеспечения информационной безопасности бизнеса находится в состоянии зарождения. Это направление несколько лучше развито в банковском секторе экономики, который в последние годы динамично растет. Финансовый сектор в своем развитии всегда ориентировался на Запад, в то время как в промышленном секторе мнения относительно направлений развития разделились. Банки без особых дискуссий следовали общемировым тенденциям в развитии своей информационной деятельности. Например, в секторе розничных операций с платежными картами практически повсеместно были внедрены программные продукты западной разработки. Это привело к наследованию соответствующих регламентов функционирования систем, в том числе и в сфере безопасности.

В промышленном и торговом секторе этого не произошло. Все чаще мы слышим о рейдерских “недружественных” поглощениях, и можно уверенно предположить, что публично-му обсуждению поддается только малая доля случаев вторжения в чужой бизнес. А любое вторжение всегда начинается с обеспечения доступа к чужой информации.

Однако вопросы информационной безопасности — это не только обеспечение конфиденциальности информации, но одновременно и контролируемое обеспечение ее доступности и целостности. По опубликованным недавно оценкам, Украина теряет 1–3 миллиарда долларов прямых иностранных инвестиций из-за отсутствия корпоративной культуры. Организация информационной безопасности на основе международных рекомендаций и сложившейся положительной практики дает возможность управления не только тем, что надо хранить, но и тем, что может и должно способствовать формированию позитивного имиджа компании у акционеров и в обществе.

В этом плане показательна волна поглощений крупных украинских банков иностранными инвесторами. Банки — единственная сфера экономики в Украине, способная разговаривать с международным бизнесом на одном языке. Наличие в банках осмысленной деятельности по обеспечению информационной безопасности является одним из существенных факторов обеспечения серьезной кооперации с мировым бизнесом.

Конечно, до появления действительно публичных компаний в Украине и формирования фондового рынка еще очень далеко. Но среднему бизнесу уже присущи все признаки рыночного функционирования и конкуренции. Рано или поздно это приведет к смене стратегий от “производит и продавать” к “воспринимать и реагировать”, как это принято во всем мире. Бизнес становится прежде всего информационным — сегодня ни размер, ни мощность предприятия не обеспечивают конкурентоспособность сами по себе. Если предприятие не способно быстро реагировать на рыночную конъюнктуру, т. е. не способно добывать информацию из всех доступных источников, в том числе у конкурентов, оно проигрывает.

Сегодня информацию классифицируют исходя из ее конфиденциальности, практически полностью игнорируя дос-

тупность и целостность. Такой подход сложился исторически, однако он не соответствует современным требованиям. Статус конфиденциальности информации является времязависимым — любая информация, даже составляющая государственную тайну, со временем теряет важность и переходит в разряд общедоступной. Бизнес-информация предприятия также со временем должна претерпевать изменение категории конфиденциальности. Но существует ли на предприятиях понятие жизненного цикла информации? Ведь информация устаревает и, следовательно, конфиденциальные отчеты, созданные вчера, и те же отчеты за позапрошлый год имеют разную важность и уровень конфиденциальности. Зачем же тратить впустую деньги, обеспечивая им одинаковую защиту? Возникает необходимость введения понятия регламента управления информационной безопасностью.

### Человеческий фактор

Аудит информационного обеспечения деятельности в лидирующих предприятиях демонстрирует, что только в единичных компаниях регламент обеспечения информационной безопасности существует хоть в каком-то виде вообще. Согласно общепринятой практике в кадровых договорах существует раздел по конфиденциальности информации. Однако прямая трактовка типичных положений этого раздела может дать основания для обвинения любого сотрудника в нарушении правил — часто в эти разделы бывает “свалено” все. С другой стороны, эти положения не имеют под собой регламентной базы, основой которой является классификация информации, циркулирующей в организации, с учетом оценки ее информационной критичности для бизнеса.

Сегодня на очень редких промышленных предприятиях утвердился и применяется регламент управления доступностью информации. Как правило, руководство пытается возложить ответственность за эту работу на ИТ-департамент. Однако это неправильно — безопасностью должны заниматься профессионально подготовленные специалисты.

Основные угрозы информационной безопасности в основном связаны с деятельностью собственного персонала. Угрозы также исходят из внешних телекоммуникационных каналов, которые могут быть подвержены несанкционированному мониторингу и атакам. По данным опроса, проведенного российской фирмой InfoWatch, более 56% атак осуществляется внутри компании. Таким образом, основного внимания требует собственный персонал — его удовлетворенность и лояльность, квалификационный уровень, мотивация и т.п. На подавляющем числе предприятий сотрудник в лучшем случае знает, что о деятельности предприятия нельзя никому ничего рассказывать и что пароли необходимо периодически менять. Вопросы парольной защиты являются слабым местом систем безопасности — часто сотрудники записывают пароли на стикерах, прикрепленных к монитору, или в других общедоступных местах.

### Методики

Система обеспечения информационной безопасности не может сводиться только к компьютерам и телекоммуникационным сетям. Из-за резкого роста объема информации, циркулирующей в цифровом виде, увеличивается значение про-

граммно-технических и организационных мероприятий по управлению доступом к информации.

Типичное предприятие обычно имеет:

- классификатор информации с указанием степени ее конфиденциальности, целостности, доступности и порядка изменения степеней этих параметров во времени;
- регламент управления информацией и обеспечения ее защиты;
- подразделение, которому поручено управление и проведение регламентных работ.

Защита информации обходится предприятиям недешево, поэтому бюджет обеспечения безопасности должен быть экономически и финансово обоснован. Бизнес должен сформировать сумму средств, которая может быть рационально потрачена на управление информацией предприятия.

Можно выделить несколько уровней защиты информации: уровень операционной системы, сетевой и телекоммуникационный уровень, уровень базы данных, уровень логики приложения, уровень интерфейса. Согласованное управление защитой информации на всех уровнях — задача, не имеющая оптимального решения. Например, уровень защиты данных, предоставляемый операционной системой, как правило, эксплуатируется при наличии “установок по умолчанию”. Большинство успешных атак добиваются цели именно благодаря этому обстоятельству.

На сетевом и телекоммуникационном уровне достигнута действительно высокая степень унификации и стандартизации. Хотя в специальных случаях на данном уровне также целесообразно воспользоваться имеющейся вариативностью.

Уровень базы данных все больше “погружается” в приложения и все менее является фактором эксплуатирующей организации. Если в начале и середине 90-х гг. в Украине не было предприятия, сотрудники ИТ-службы которого не разрабатывали бы “свой R/3” или хотя бы “свою 1С”, то сегодня большинство компаний используют индустриальные решения.

На уровне базы данных в основном оперируют разработчики, поэтому информационные аспекты безопасности при взаимодействии с пользователем переносятся на бизнес-логику программных приложений.

Уровень информационной защиты программных приложений является наименее стандартизированной частью и будет оставаться таким и впредь. Однажды в начале 90-х годов в Швейцарии спросили работника безопасности одного из банков: “А можно ли ознакомиться со стандартами информационной безопасности программных приложений?” Ответ был неожиданным: “Таких стандартов просто не может быть: стандарт “замка” одновременно описывает стандарт “ключа” и “отмычки””.

К сожалению, возможности, предоставляемые программными приложениями на этом уровне, часто не могут соответствовать реальным потребностям предприятия. Это связано, например, с наличием возможности настройки сложных правил обеспечения доступа к информации, с требованиями одновременно учитывать селективность (по контрагентам, по деятельности, по лимитному размеру сумм, по регионам и т.п.). В некоторых случаях

возникает потребность управления доступностью исторических бизнес-данных предприятия.

### Вместо заключения

Основная проблема в формировании стратегии информационной безопасности сегодня состоит в том, что бизнес не понимает всей серьезности создавшейся ситуации и пытается решить ее “малой кровью” за счет того, что передоверяет решение задачи отделам ИТ. Эта стратегия неправильная: во-первых, ИТ-отделы решают проблемы безопасности при наличии свободного времени и свободных средств, а во-вторых, слишком увлекаются техническими средствами. Наконец, возникает организационная сложность, связанная с тем, что некому проверить постановку задач по информационной безопасности и корректность их решения.

В идеале на предприятии должны существовать три самостоятельных подразделения: департамент ИТ, отдел информационной безопасности и секторы аудита ИТ и аудита ИБ в отделе аудита компании, которые занимались бы проверкой соответствующих подразделений. Однако здесь возникает целый ряд сложных вопросов, причем главный из них — кадры, ведь не секрет, что специалистов по информационной безопасности сейчас практически нет, поскольку ВУЗы их не готовят.

Если в ближайшее время положение на рынке информационной безопасности предприятий кардинально не изменится в лучшую сторону, то вопросы обеспечения информационной безопасности национального бизнеса могут постепенно перейти в плоскость национальной безопасности.

*Владимир Безмальный,  
“БМС Консалтинг”, консультант  
по вопросам информационной  
безопасности Сергей Корнеев,  
PMCG, директор*

## НОВОСТИ

### ПРОЕКТЫ

#### Cisco строит оптическую сеть для “Укртелекома”

Транспортные мощности “Укртелекома” пополнятся второй очередью оптической DWDM-сети, в основу которой положена мультисервисная транспортная платформа Cisco ONS 15454 MSTP. Новая сеть DWDM дает “Укртелекому” широкие возможности по предоставлению различных услуг, связанных с высокоскоростной передачей данных, на всей территории Украины. Уникальность проекта состоит и в том, что Cisco впервые в странах СНГ выступила как системный интегратор, реализовав проект “под ключ” на основе прямого договора с ОАО “Укртелеком”. В рамках проекта специалисты ОАО “Укртелеком” прошли обучение по оптическим технологиям Cisco и теперь могут самостоятельно планировать ее дальнейшее развитие.

Новая сеть построена на базе технологии спектрального уплотнения каналов DWDM (Dense Wavelength Division Multiplexing), которая обеспечивает мультиплексирование и прозрачный транспорт нескольких потоков из разных источников.