

## ПРИНЦИПЫ ПОЛИТИКИ ИНФОБЕЗОПАСНОСТИ БАНКА: ЗАКОННОСТЬ И АДЕКВАТНОСТЬ

На мой взгляд, не существует сколько-нибудь весомых факторов, сдерживающих развитие систем информационной безопасности в банках в глобальном масштабе. Банки очень чутко осознают критичность процессов, связанных с ИБ. Сложности в развитии и реализации ИБ в банках, зачастую, связаны с немалым числом требований нормативной базы к банковским структурам в части обеспечения ИБ. К слову, во многих банках данные процессы протекают в плановом режиме, наряду с модернизацией смежных процессов.

Возросла степень осознания всей важности развития ИБ и в небанковских компаниях. Объясняется это лишь одним фактором - требованиями бизнеса. Число угроз ИБ не стало больше, а вот возможности потенциальных злоумышленников заметно выросли. Еще одной причиной роста значимости решения вопросов ИБ является как укрупнение размеров инфосистем, так и увеличение требований к качеству предоставляемых сетевых сервисов. Практика показала, что грамот-

ное развитие сетевых сервисов всегда проводится с учетом решения вопросов, связанных с ИБ.

Спектр решений по ИБ сильно вырос и качественно изменился. На сегодня ИТ-интеграторы предлагают целые "пакеты решений по ИБ" для различных вертикалей рынка. Кроме того, при разработке масштабных проектов хорошей практикой является проведение ряда научно-исследовательских работ (аудита, препроектного обследования, построения пилота и др.) с целью выявления подлинных проблем и нужд заказчика. Полученные данные приводят к разработке гранулированного подхода и к успешной реализации проектов по ИБ.

Можно выделить два достаточно простых принципа, на которых должна базироваться политика информационной безопасности банка: адекватность и законность. Первый принцип подразумевает создание непротиворечивой политики ИБ, отвечающей целям бизнеса организации. Реализация второго принципа позволяет регламентировать процесс внедрения и модернизации систе-

мы ИБ. Именно гласность и законность позволят не только получить поддержку руководства в ряде действий, но и заложат фундамент для дальнейшей работы в части ИБ.

При этом необходимо добиться внедрения прозрачной системы контроля работы пользователей. В настоящее время существует множество комплексных и отработанных решений в этом направлении: централизованные системы контроля работы приложений на АРМх пользователей, централизованные системы мониторинга и корреляции событий безопасности, системы контроля и фильтрации контента и др. Важно, чтобы до пользователей было доведено, что данные системы внедрены в организации и успешно эксплуатируются службами информационной безопасности и внутреннего контроля.

На полноту и эффективность работы системы обеспечения ИБ влияет также и степень осведомленности сотрудников соответствующих подразделений банка (ИТ-подразделения, службы безопасности, службы внутреннего кон-



Андрей Бедрань,  
Департамент  
информационной безопасности  
ЗАО "Энвижн Груп"

троля) об уязвимостях тех или иных критичных ресурсов организации. Хорошей практикой является проведение комплексного аудита ИБ и ряда инструментальных проверок защищенности сетевых сегментов. Более того, только регулярная переоценка внедренных процессов обеспечения ИБ позволит убедиться в адекватности выбранных мер защиты. Данные работы способны выявить изменения, произошедшие с момента проведения предыдущего аудита, а также покажут степень соответствия производимых интеграционных процессов выбранной стратегии развития.

## ГДЕ ГРАНИЦЫ ЧАСТНОЙ ЖИЗНИ?



Михаил Калининко,  
генеральный директор  
компании "StarForce"

Сегодня одной из насущных проблем в развитии систем инфобезопасности являются законодательные ограничения, связанные с защитой частной жизни, установленные в большинстве развитых стран. Это либо неопределенность понятия "частная жизнь" в контексте действий сотрудников на рабочем месте, либо слишком широкая трактовка понятия "личная информация". Где провести границу между тайной личной жизнью и информацией, которую сотрудник обрабатывает в рамках служебных обязанностей? Например, каким образом можно разделить частную и служебную переписку при контроле электронной почты? Поэтому подходы к обеспечению

информационной безопасности, связанные с ограничением доступа или контролем информационных потоков, с которыми работает или которые создает сотрудник, балансируют на тонкой грани между вмешательством в частную жизнь и защитой конфиденциальной информации.

Таким образом, прежде всего, необходимо определить границы понятия "частная жизнь", которые соответствуют законодательству страны. Далее, в рамках контроля служебных функций, основной мерой обеспечения безопасности должно стать протоколирование действий сотрудника и их сравнение с его служебными обязанностями. Без возможности контроля действий сотрудника вопроса обеспечения безопасности, на мой взгляд, неактуален.

Тем временем, обеспечение безопасности информационных систем и данных становится жизненно необходимым. Поскольку работа с клиентами все более и более уходит в электронный формат, защита данных клиентов и доступа к возможностям осуществления транзакций непосредственно влияет на жизнь как самого банка, так и клиента. Информационная безопасность автоматически становится эквива-

лентна финансовой безопасности, защите от воровства денег.

В ряде стран вводится юридическая и финансовая ответственность для компаний и топ-менеджмента за нарушения защищенности конфиденциальных данных своих клиентов. В известных случаях, когда из-за неосторожных действий сотрудников в общем доступе оказывались данные клиентов с номерами их кредитных карт, их обнародование приводило к штрафам и к существенному ущербу для деловой репутации банка. Поэтому для обеспечения информационной безопасности в банке нужно использовать специализированные решения, предназначенные для финансовой сферы, ограничивающие права доступа к отдельным частям системы, к документам и так далее.

Для повышения адекватности системы информационной безопасности требованиям бизнеса, на мой взгляд, её необходимо включать составной частью в операционную деятельность банка, в увязку с остальными показателями его работы. Это можно сделать путем включения соответствующих показателей в систему ключевых индикаторов производительности (KPI), либо используя любые другие системы и методологии организационного развития компании.

В этом случае появляется возможность перейти от технических описаний систем безопасности к их функциональным описаниям в бизнес-понятиях и бизнес-категориях, идти не от внедрения технологий "вверх" к решению задач, а "вниз", от бизнес-задач к технологиям: сначала ставится бизнес-задача, а потом подбирается решение, которое будет решать именно её.

В целом же основополагающим принципом осуществления мер информационной безопасности в банке должен стать принцип разумной достаточности. В частности, разработанные стандарты политики безопасности для различных сотрудников банка должны быть соизмеримы с их задачами. В остальном общие подходы остаются прежними: разграничение доступа, контроль соответствия действий сотрудников служебным обязанностям, защита доступной сотрудникам информации как при помощи средств информационной безопасности, так и с помощью организационных и иных мер.

В целом основным условием информационной безопасности является определенность и регламентированность бизнес-процессов. Чем стандартнее бизнес-процессы, тем безопаснее можно сделать систему.