



Мнение экспертов о проблемах информационной безопасности в банковской сфере (выдержки из отчета)

На сегодняшний день ситуация в банковской сфере такова, что зачастую ни руководители банков, ни специалисты служб безопасности, ни сотрудники IT-отделов не имеют четкого представления о том, какая именно информация в банке имеет ценность для конкурентов и подлежит особо тщательному контролю. Также в любом банке присутствуют информационные потоки, которые как бы не существуют официально, но в реальности могут представлять угрозу безопасности – к примеру, неформальное внутреннее общение сотрудников банка или поиск ими новой работы. Между тем, утечки из банка конфиденциальной информации способны не только ослабить его позиции в конкурентной борьбе, но и существенно ухудшить отношение к этому банку со стороны клиентов и государственных структур. В этом плане наиболее опасной оказывается утечка данных о клиентах (как частных, так и корпоративных) и/или о проводимых ими финансовых операциях. Со всеми вышеописанными проблемами уже давно столкнулись европейские и американские банки, а в последние годы – также банки России и других стран СНГ.

Сегодня западные капиталы активно приходят на российский рынок банковских услуг, а с ними – и их практики ведения бизнеса, включающие в себя элементы информационных войн (промышленный шпионаж, переманивание клиентов и сотрудников и т.д.). В таких условиях внедрение комплексных систем информационной безопасности становится очень актуальным.

На первый план выходит противодействие инсайдерам. К их числу обычно относят:

- просто недобросовестных сотрудников;
- сотрудников, имеющих контакты с криминальными структурами;
- сотрудников, сознательно работающих на банки-конкуренты (нанятых или засланных ими);
- сотрудников, обиженных на начальство и потому скрытно вредящих банку, без выгоды для себя.

Специалисты по банковской безопасности особо выделяют следующий перечень угроз информбезопасности (утечек):

1. Утечка кадров к конкурентам. Уходящие специалисты обычно уносят с собой разного рода конфиденциальную информацию – например, обсуждаемые бизнес-идеи, применяемые технологии, данные о ключевых клиентах и т.д. В таких случаях для службы безопасности особенно важно перехватить момент, когда сотрудник начинает рассылать резюме, обсуждать в чате переход на другую работу или сам получает e-mail с предложением о работе от конкурентов. Такому сотруднику имеет смысл тут же перекрыть доступ к конфиденциальной информации банка.

2. Утечка информации по корпоративным клиентам. Обычно с крупными корпоративными клиентами банки работают индивидуально – на особых условиях. Если эти условия становятся известны конкурентам, те могут попросту переманить корпоративного клиента, предложив более выгодные условия сотрудничества.

3. Утечка информации о проводимых банковских транзакциях – кто, куда и какие суммы переводит. Практически всегда обнародованный факт такой утечки приводит к фатальному оттоку клиентов и подрыву доверия к банку. В таких ситуациях особенно важно следить за персоналом. К примеру, сформировавшаяся связка операционистки и менеджера может «слить» очень много информации о проводимых операциях.

4. Очень много информации конкурентам и просто недоброжелателям может дать внутренняя служебная переписка – обсуждение проблем в коллективе, чьих-то ошибок и т.д. Обычно она ведется во внутреннем чате или с использованием программ типа ICQ. При этом доступ к секретной информации могут получать сотрудники, изначально такого доступа не имевшие. Со всеми вытекающими последствиями.

5. Утечки в прессу. Без комментариев.

6. Утечка информации о разрабатываемых маркетинговых программах, инновациях в этой сфере. В результате многомесячная работа и затраты на нее могут оказаться бесполезными, когда банк-конкурент

Это ваша власть
над информацией



выведет эту программу на рынок чуть-чуть раньше, просто украв ее у реальных разработчиков. К слову, это часто встречающаяся ситуация.

8. Утечка информации об инвестиционных планах банка. Способна привести к срыву важных и потенциально очень доходных проектов.

9. Утечка информации о системе безопасности банка. Открывает широкие возможности для деятельности криминальных структур.

10. Утечки информации о перемещениях наличных денег (включая выдаваемые наличными кредиты). Следствием может стать банальное ограбление инкассаторов или клиентов.

Для справки:

Рекомендации по стандартизации Банка России в области обеспечения информационной безопасности предусматривают следующие частные политики информбезопасности банка:

- политика использования электронной почты и ресурсов сети интернет;
- политика по обеспечению информбезопасности средствами антивирусной защиты;
- политики мониторинга и менеджмента инцидентов информационной безопасности;
- политика по обеспечению информбезопасности при управлении доступом и регистрации;
- политика по обеспечению информбезопасности при назначении и распределении ролей и обеспечении доверия к персоналу;
- политика по обеспечению информбезопасности банковских платежных технологических процессов;
- политика по обеспечению информбезопасности банковских информационных технологических процессов.