

О. А. ТАРАСОВ

*доцент кафедры математических методов, статистики
и информационных технологий в экономике,
кандидат физико-математических наук*

«Не кради» (Исх. 20:15)

*Уволиться из компании, прихватив с собой базу
данных клиентов, сегодня в России считается
хорошим тоном и чуть ли не доблестью [1]*

ОЦЕНКА СТОИМОСТИ УЩЕРБА ОТ РАЗГЛАШЕНИЯ КЛИЕНТСКОЙ БАЗЫ ДАННЫХ БАНКА

Важнейшей задачей отечественного бизнеса при вступлении России во Всемирную торговую организацию является повышение его конкурентоспособности. Одной из составляющих конкурентоспособности выступает информационная безопасность.

В кризис уберечь тайны намного сложнее. Сокращение штата, снижение зарплат, невыплата бонусов подталкивают людей к поиску других источников дохода, в том числе и нелегальных.

Так, даже в докризисный 2005 г. все без исключения крупные западные банки зафиксировали утечки информации, причем 72% из них потеряли в результате более 1 млн USD [1]. В том же году

произошли утечки в 96% крупных российских компаниях, но большинство их руководителей не подозревало об этом, т. к. лишь 2% российских компаний использовало специальные системы информационной защиты [1].

Сейчас ситуация только ухудшилась, поскольку российские компании сократили расходы на информационную безопасность [2]. И это притом, что по российской и международной статистике 62-64% информации крадется собственными сотрудниками организации [1], [2]¹.

В 93% случаев крадут персональные данные, в 6% — ноу-хау, а в 1% — другую информацию [5]. Объектом преступления в 58% случаев становятся коммерческие предприятия, в 22% — государственные органы и в 20% — общественные объединения, учебные заведения и др. [5].

Выполним оценку ущерба от разглашения клиентской базы данных (КБД) банка при условиях, что средства клиентов не были похищены, банк не выплачивал клиентам компенсацию за утечку их персональных данных² и не привлекал сторонние средства взамен средств ушедших от него клиентов. Тогда банк ожидают следующие последствия:

- 1) необходимо изменить информацию в КБД;
- 2) необходимо переизготовить пластиковые карты;
- 3) часть клиентов откажется от услуг банка, что повлечет уменьшение его прибыли;
- 4) можно вернуть часть ущерба через суд.

Следовательно, величина ущерба $У$ банка будет составлять:

$$У = ЗКБД + ЗП + УП - ШН,$$

где ЗКБД — затраты на изменение КБД, ЗП — затраты на переизготовление пластиковых карт, УП — упущенная прибыль, ШН — штраф нарушителя прав банка.

¹ Классический пример — кража клиентской базы данных из инвестиционного банка Morgan Stanley в 2007 г., в которой оказалась виновна бывший консультант банка И. Чиловиц, решившая открыть собственную консалтинговую фирму [3]. Установка почтового фильтра просто исключила бы возможность этого инцидента [4].

² Впрочем, российские банки не особенно стремятся выплачивать даже похищенную со счетов клиента сумму. Так, при хищении денег с пластиковой карточки только 15% владельцев смогли вернуть полную сумму пропажи, еще 19% получили частичную компенсацию, а остальные 66% остались ни с чем [6].

Расчет затрат на изменение базы данных представлен в табл. 1.

Таблица 1

Затраты на изменение клиентской базы данных

Содержание затрат	Размер затрат, руб.
Заработная плата персонала, включая налоги	30000
Амортизация оборудования (компьютеры, оргтехника)	1000
Оплата доступа в Интернет	1000
Оплата информационных ресурсов (электронные и бумажные издания и т. п.)	1000
Содержание офиса	3000
Всего затраты на изменение базы данных	36000

Оценим теперь стоимость замены пластиковых карт. Печать карты одним цветом стоит 0.45 USD; печать дополнительным цветом прибавляет к стоимости 0.09 USD [7]. Прочие расходы на изготовление одной карты будут около 0.18 USD. При курсе 1 USD = 27.98 руб. на 01.06.2011 [8] и использовании семи цветов, цена карты равна:

$$(0.45 + 0.09 \cdot 6 + 0.18) \cdot 27.98 = 32,74 \text{ руб.}$$

Предположим, что услугами банка пользуются 800 тысяч клиентов. Тогда стоимость переизготовления пластиковых карт будет равна:

$$800\,000 \cdot 32,74 \approx 26\,189\,000 \text{ руб.}$$

Согласно ч. 2 ст. 15 ГК РФ [9], упущенная выгода — это неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

Рассчитаем упущенную выгоду вследствие отказа части клиентов от услуг банка. Примем, что чистая прибыль банка за год составила $P = 1000$ млн руб. Согласно исследованиям Ponemon Institute [5], $d = 25\%$ клиентов либо сразу отказываются от услуг ненадежной фирмы, либо делают это в ближайшем будущем¹ (рис. 1). Следовательно, при опубликовании КБД банка, его упущенная выгода на конец первого года будет $1000 \text{ млн} \cdot 0,25 = 250 \text{ млн руб.}$

¹ Этот вывод согласуется со случаем утечки информации в британском банке HSBC. За три года из 24 тыс. клиентов, у которых были похищены персональные данные, покинули банк 9 тыс. (или 37.5%) [10].



Рис. 1. Реакция клиентов на раскрытие коммерческой тайны организации [5]

Предположим, что клиенты, покинувшие банк, не вернуться; рост клиентуры банка за счет других лиц, не знающих о факте хищения КБД, будет составлять $r = 5\%$ в год, начиная со второго года с даты утечки информации; а ставка дисконтирования в год будет $I = 10\%$. Тогда банк восстановит чистую годовую прибыль через $25\%/5\% = 5$ лет, и величина современной стоимости его упущенной прибыли на начало первого года (на дату утечки информации) будет определяться как

$$\sum_{n=1}^5 \frac{P(d - r(n-1))}{(1+i)^n} = 1000 \text{ млн руб.} \times \sum_{n=1}^5 \frac{(0,25 - 0,05(n-1))}{(1+0,1)^n} =$$

$$= 604,606 \text{ млн руб.}$$

Согласно ч. 3 ст. 183 УК РФ, за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, причинившие крупный ущерб или совершенные из корыстной заинтересованности, может быть назначен штраф до 200 тыс. руб. [11].

Тогда величина ущерба от разглашения КБД банка будет равна:
 $У = 36\,000 + 26\,189\,000 + 604\,606\,000 - 200\,000 = 630\,631\,000$ руб.
 или 63% от чистой годовой прибыли банка до момента разглашения его коммерческой тайны.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальность проблем обеспечения внутренней информационной безопасности [Электронный ресурс]. Режим доступа: http://www.aferizm.ru/bb/it/bb_it_aktyalno_infbez.htm от 23.10.2006.

2. Садыков А. Уходя — уноси [Электронный ресурс]. Режим доступа: http://www.trud.ru/article/05-12-2008/136091__uxodja--unos.html от 15.12.2008.
3. 26 лет тюрьмы дали инсайдеру, укравшему клиентскую базу Morgan Stanley [Электронный ресурс]. Режим доступа: <http://www.securitylab.ru/news/290548.php>. от 07.02.2007.
4. Morgan Stanley продолжает отлавливать инсайдеров [Электронный ресурс]. Режим доступа: <http://www.sarg.ru/article.aspx?id=17674&iid=817> от 02.05.2007.
5. Значение репутации банка [Электронный ресурс]. Режим доступа: <http://www.klerk.ru/bank/fin/?45166#>.
6. Мошеники ограбили клиентов Банка Москвы на 1,6 млн руб [Электронный ресурс]. Режим доступа: <http://www.rb.ru/topstory/incidents/2010/04/05/082624.html> от 05.04.2010.
7. Пашковская С. В. Пластиковые деньги тоже надо делать. Что надо знать о пластиковых карточках [Электронный ресурс]. Режим доступа: http://publish.ruprint.ru/stories/8/123_1.php от 16.08.2004.
8. Центральный банк Российской Федерации. Курсы валют [Электронный ресурс]. Режим доступа: http://www.cbr.ru/currency_base от 01.06.2011
9. Гражданский кодекс Российской Федерации. Часть 1. от 30.11.1994 № 51-ФЗ [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/popular/gkrf1/> (ред. от 06.04.2011).
10. Британский банк признался в утечке информации о 24 тысячах клиентов [Электронный ресурс]. Режим доступа: <http://www.lenta.ru/news/2010/03/11/hsbc/> от 11.03.2010.
11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/popular/ukrf/> ред. от 04.05.2011.