ИНСАЙДЕР – УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

Напора И. Ю. (Черкасский национальный университет им. Б. Хмельницкого, г. Черкассы, Украина)

На информационную безопасность банка влияют как внешние, так и внутренние угрозы. В течении многих лет банки вели работу по борьбе с внешним несанкционированным доступом и совсем упустили из поля зрения главную опасность – собственного сотрудника-внутреннего нарушителя, который имеет доступ к информации. Когда говорим о киберпреступности в банковской сфере, то, как правило, мы обращаем внимание на внешние угрозы и забываем об инсайдерах.

Сотрудник банка в той или иной мере имеет доступ к конфиденциальной информации, а значит, является источником риска ее утечки или порчи.

К сожалению, большую часть субъектов несанкционированного доступа составляет персонал, который имеет доступ к информации и знаком с технологией ее обработки. Среди нарушителей встречаются и те, кто сам должен отвечать за информационную безопасность банка.

Информационная безопасность – один из основных вопросов для банковской сферы, поскольку банк выступает как доверенное лицо своих клиентов, которое обладает конфиденциальными сведениями об их финансовой и коммерческой деятельности.

Инсайдер (от англ. *inside* – внутри) – любое лицо, имеющее доступ к конфиденциальной информации о делах фирмы благодаря своему служебному положению и родственным связям [1].

Согласно Инструкции о порядке регулирования деятельности банков в Украине, инсайдер – лицо, которое благодаря своему служебному положению или родственным связям имеет доступ к конфиденциальной информации о деятельности банка, недоступной широкой общественности, и может использовать ее в собственных целях для обогащения, получения неконкурентных преимуществ, привилегий и т. д. [2].

Существует несколько подходов к классификации внутренних нарушителей (инсайдеров). Компания IDC рассматривает такие группы инсайдеров, как граждане, нарушители, отступники, предатели. Недостатком этой классификации есть простое распределение сотрудников по группам в зависимости от того, чем они занимаются на рабочем месте. Более полная классификация, основанная на анализе защиты данных от утечки, уничтожения и искажения, принадлежит компании InfoWatch. Она выделяет следующие типы внутренних нарушителей: халатный, манипулируемый, обиженный, нелояльный, подрабатывающий, внедренный [3, с. 17–18].

Для выявления «возможного инсайдера» используют механизм комплексного подхода к анализу сотрудников, который состоит в исследовании информации с предыдущего места работы и особенности прихода сотрудника в организацию, психологического портрета, особенностей поведения на рабочем месте, наличия проблем в повседневной жизни и степени допуска к конфиденциальной информации [4, с. 19].

Аналитики считают, что утечка информации происходит в основном из-за инсайдеров, которые готовы продать информацию, болтливости персонала, подкупа сотрудников банка, проникновения в базы данных [5].

Повышенное внимание к внутренним угрозам информационной безопасности, прежде всего, обусловлено тем, что инсайдерские инциденты происходят намного чаще, чем внешние атаки, но банки стараются не афишировать внутренние проблемы. Разглашение конфиденциальной информации чаще всего происходит из-за того, что руководство банков не уделяет должного внимания угрозам утечки информации, связанной с персоналом. Игнорирование этих угроз приводит к серьезным последствиям, и речь идет не только о финансовых потерях, но и о снижении имиджа банка, поскольку он не может защитить как свою конфиденциальную информацию, так и информацию клиентов.

Очень часто сотрудники банка становятся «поставщиками» конфиденциальной информации из-за собственной халатности, но самая серьезная проблема – персонал банка, который сознательно продает данную информацию.

Литература

1. *Райзберг, Б. А.,* Современный экономический словарь / Б. А. Райзберг, Л. Ш. Лозовский, Е. Б. Стародубцев. – 2-е изд., испр. – М. : Инфра-М, 1999. – 479 с.
2. Інструкція про порядок регулювання діяльності банків в Україні [Електронный ресурс // Постанова Правління Національного банку України від 28.08.2001 р. № 368]. – Режим доступа: http://www.bank.gov.ua/control/uk/publish/article?art_id=123342&cat_id=123215
3. *Скиба, Б. Ю.* Руководство по защите от внутренних угроз информационной безопасности / Б. Ю. Скиба, Б. А. Курбатов. – М. : Питер, 2008. – 320 с.
4. *Снегуров, А. В.* Подход к повышению эффективности выявления инсайдеров при обеспечении информационной безопасности организации / А. В. Снегуров, А. Д. Кравченко, Е. А. Ткаченко // Восточно-Европейский журнал передовых технологий. – 2011. – № 2/9 (50). – С. 17–20
5. Аналитические данные [Електронный ресурс]. – Режим доступа: http:// www.infowatch.ru.