УДК 33

Угрозы информационной безопасности банков, связанные с использованием социальных сетей

Ненашев Сергей Михайлович

Аспирант,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, просп. Ленинградский, 49;
e-mail: snenashev@gmail.com

Аннотация

Социальные сети представляют собой прямой, быстрый и практически бесплатный канал связи с клиентами, поэтому интерес российских и зарубежных банков к ним постоянно растет. Присутствие банков в социальных сетях создает специфические угрозы информационной безопасности банка и его клиентов. В статье рассматриваются некоторые из таких угроз и предлагаются способы противодействия им. Автор отмечает, что предприятиям финансового сектора, традиционно прилагающим значительные усилия к обеспечению собственной информационной безопасности, необходимо учитывать все возможные угрозы безопасности, связанные с использованием социальных сетей, в политике информационной безопасности и в планах развития информационной инфраструктуры предприятия. Для противодействия социальной инженерии, направленной против клиентов банков, следует более активно информировать клиентов о всех возможных угрозах, а также исключить социальные сети из числа явных каналов связи между сотрудниками, допускаемых политикой информационной безопасности для обмена любой информацией, имеющей отношение к деятельности банка.

Для цитирования в научных исследованиях

Ненашев С.М. Угрозы информационной безопасности банков, связанные с использованием социальных сетей // Экономика: вчера, сегодня, завтра. 2019. Том 9. № 4А. С. 17-23.

Ключевые слова

Банк, угроза информационной безопасности, клиент, социальная сеть, канал связи, финансовый сектор.

Введение

Банковская деятельность связана с обработкой больших объемов информации, основную часть которых составляют конфиденциальные данные клиентов. К ним относятся личные данные пользователей, копии их документов, номера счетов, данные о проведенных операциях, транзакциях и пр. В процессе работы с этой информацией важно, чтобы она не попала в руки злоумышленников, не была изменена или утеряна. Учитывая важность архивов, хранимых в информационной среде банка, существенно возросла их ценность и требования к защите банковской информации.

Сегодня интерес как российских, так и зарубежных банков к социальным сетям в значительной мере вырос. Социальные сети для банков являются каналом взаимодействия с клиентами. Некоторые банки используют сети для круглосуточной клиентской поддержки, проводят опросы среди подписчиков. Однако предприятиям финансового сектора, традиционно прилагающим значительные усилия для обеспечения собственной информационной безопасности, необходимо учитывать угрозы безопасности, связанные с использованием социальных сетей, в политике информационной безопасности и в планах развития информационной инфраструктуры предприятия.

Банки в социальных сетях

Интерес коммерческих банков к социальным сетям, чья популярность неуклонно растет, закономерен. В настоящее время 60% из 200 крупнейших международных банков ведут официальную страницу в социальной сети Facebook [Miranda, Chamorro, Rubio, Morgado, 2013]. Исследование официального[1] присутствия российских банков из топ-100 по показателю «Активы нетто» (источник рейтинга – banki.ru) в крупнейшей российской социальной сети «ВКонтакте» показало схожий результат: в социальных сетях представлен 61% банков, входящих в топ-100 (для топ-50 этот показатель несколько выше – 68%).

Для понимания того, какие типы сообщений банковские учреждения публикуют в социальных сетях, мы проанализировали публикации в официальных группах банков[2] в социальной сети «ВКонтакте». Результаты исследования приведены на рисунке 1.

В первую очередь банки используют социальные сети в качестве рекламной площадки. Кроме прямых рекламных сообщений, применяются и косвенные способы привлечения внимания к публикациям, например специально подготовленные вызывающие интерес изображения, не выглядящие как реклама. Банки информируют клиентов об угрозах информационной безопасности, но доля подобных сообщений крайне мала по сравнению с долями иных тематик.

Аудитории официальных банковских групп в социальных сетях продолжают расти, а банки – осваивать этот канал взаимодействия с клиентами, используя новые функции социальных сетей. Например, некоторые банки используют сервис «Товары» социальной сети «ВКонтакте» для продвижения продуктов и услуг, отвечают в социальных сетях на обращения (жалобы и

[1] Учтены только официальные группы банков в социальной сети (подтвержденные группы и группы, на которые ссылается официальный сайт банка).

[2] Рассматривались темы публикаций в официальных группах банков из топ-10 по показателю «Активы нетто» по версии banki.ru в социальной сети «ВКонтакте».

предложения) пользователей. Можно предположить, что новые возможности социальных сервисов по мере их совершенствования будут также применяться банками для решения различных задач.

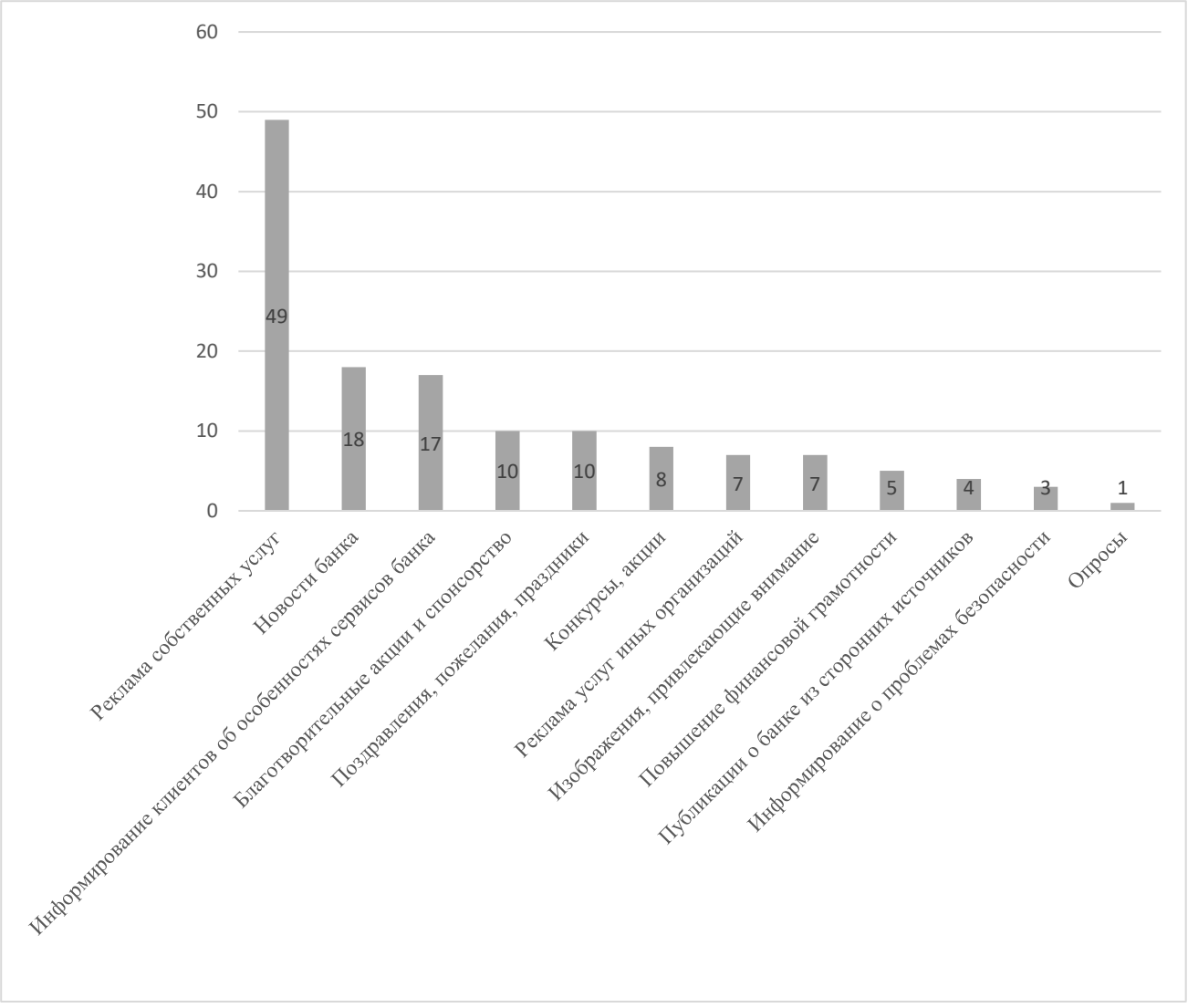

Рисунок 1 - Темы публикаций в официальных группах банков в социальных сетях

Угрозы информационной безопасности банков, возникающие вследствие использования социальных сетей

В [Ненашев, 2016] рассмотрены специфические виды угроз информационной безопасности, связанные с использованием социальных сетей, и даны общие рекомендации по противодействию им. Перечень типов подобных угроз, рассмотрение которых актуально при анализе защищенности банков и их клиентов, включает следующее:

– социальная инженерия (в том числе с использованием взломанных учетных записей и ложных личностей);
– пассивный сбор данных ограниченного доступа с использованием ложных личностей;
– дезинформирование пользователей;

– имитация массовости мнения или действия в целях информационно-психологического влияния на пользователей социальных сетей.

Угрозы социальной инженерии в отношении клиентов банковских учреждений могут реализовываться следующими путями:

– получение злоумышленником платежной информации клиентов с использованием взломанной учетной записи (например, просьба о совершении платежа со взломанной учетной записи супруга или супруги);
– провоцирование платежа путем распространения некоторой публикации взломанными учетными записями или ложными личностями; подобные публикации могут рассылаться с помощью личных сообщений или как «репост» (например, публикация группой ложных личностей сообщений о сборе пожертвований);
– получение злоумышленником сведений, составляющих коммерческую или банковскую тайну, путем злоупотребления доверием сотрудника банка (например, с помощью отправки некоторого сообщения сотруднику банка с использованием взломанной учетной записи его непосредственного руководителя).

Пассивный сбор данных ограниченного доступа с использованием ложных личностей – часть подготовки к применению социальной инженерии. Присутствие в социальных сетях осуществляется банками через создание официальной группы, подписчиками которой становятся в основном клиенты банка. Это означает, что злоумышленник может составить обширный список клиентов некоторого банковского учреждения (например, одна из таких официальных групп в социальной сети «ВКонтакте» насчитывает более 2,5 миллионов подписчиков). Для значительной части списка подписчиков имеется возможность получения номера мобильного телефона и другой личной информации (в том числе через атаки на приватность скрываемых сведений), которая может применяться при осуществлении социальной инженерии.

Добывание подобных сведений может выполняться с помощью собственных или взломанных учетных записей или ложных личностей. Указанные действия могут осуществляться не только злоумышленниками, но и конкурентами банка.

Дезинформирование пользователей вне рамок социальной инженерии чаще всего является элементом конкурентной борьбы финансовых учреждений или иных общностей. Дезинформирование комбинируется с имитацией массовости и социальной инженерией. Второго декабря 2016 года пресс-служба ФСБ России сообщила, что «иностранные спецслужбы планируют масштабные кибератаки с целью дестабилизации финансовой системы Российской Федерации». Одним из элементов данной операции должны были стать «массовая рассылка SMS-сообщений и публикаций в социальных сетях (блогах) провокационного характера в отношении кризиса кредитно-финансовой системы России, банкротства и отзыва лицензий у ряда ведущих банков федерального и регионального значения» [ФСБ России предупредила пользователей соцсетей…, www].

Ассоциация российских банков сообщила, что ожидающиеся публикации должны «сеять панику и призывать к массовому закрытию депозитов». Также АРБ отмечает, что «злоумышленниками может распространяться ложная информация об отсутствии наличности в банкоматах некоторых банков, об "утечке информации" о введении ограничений на выдачу денежных средств и закрытии отделений некоторых банков, о получении от якобы достоверных источников информации о скачках курса рубля и о планируемом ограничении выдачи валюты. Эта недостоверная информация может сопровождаться комментариями от якобы

взволнованных граждан, подтверждающих эту ложную информацию» [Калюков и др., 2016, www].

Похожая атака была проведена в феврале 2014 года на три крупнейших банка Казахстана. В результате паники вкладчиков, спровоцированной SMS-сообщениями, сообщениями в WhatsApp и социальных сетях, «Альянс-Банк» потерял около 31% вкладов, Kaspi Bank – около 17%, «Банк ЦентрКредит» – примерно 15% [Колимечков, 2016, www].

Подходы к противодействию специфичным угрозам со стороны социальных сетей

Для противодействия социальной инженерии, направленной против клиентов банков, на наш взгляд, банкам следует, во-первых, более активно информировать клиентов об угрозах данного типа. Анализ показал, что информация об угрозах данного рода редко встречается в публикациях в официальных группах банков в социальных сетях. Во-вторых, мы рекомендуем явным образом исключить социальные сети из числа каналов связи между сотрудниками, допускаемых политикой информационной безопасности для получения задач или обмена любой информацией, имеющей отношение к деятельности банка.

Угрозы, связанные со сбором личных данных пользователей социальных сетей, являющихся клиентами банков, в первую очередь связаны с возможностью установить со значительной степенью уверенности, что некоторое лицо является клиентом банка по факту подписки пользователя социальной сети на официальное сообщество банка в социальной сети. Следовательно, имеет смысл закрыть список подписчиков официальных групп банков от просмотра любыми пользователями в социальных сетях, обеспечивающих такую возможность.

Дезинформирование пользователей и попытки манипулирования их мнением средствами социальных сетей чаще всего не оказывают существенного влияния на деятельность финансовых учреждений, однако порой это влияние может быть весьма серьезным, поэтому необходимо на постоянной основе отслеживать публикации с упоминанием банка, оценивать потенциал распространения публикаций [Ненашев, 2019] и степень их потенциальной опасности и реагировать на угрожающие публикации, имеющие значительный потенциал распространения, публикуя опровержения или иные сведения, соответствующие содержанию вредоносной публикации [Новиков, Бандурко, 2015].

Заключение

Таким образом, социальные сети играют важную роль в современной жизни, однако некоторые угрозы, связанные с их применением в бизнесе, сегодня осознаются недостаточно хорошо в силу относительной краткости периода активного использования социальных сетей. Социальные сети представляют собой прямой, быстрый и практически бесплатный канал связи с клиентами, поэтому присутствие банков в них растет, что, однако, создает специфические угрозы информационной безопасности банка и его клиентов. Предприятиям финансового сектора, традиционно прилагающим значительные усилия к обеспечению собственной информационной безопасности, необходимо учитывать возможные угрозы безопасности, связанные с использованием социальных сетей, в политиках информационной безопасности и в планах развития информационной инфраструктуры предприятия.

Библиография

1. Калюков Е. и др. ФСБ сообщила о подготовке иностранными спецслужбами кибератаки на банки. РБК. 2016. URL: https://www.rbc.ru/finances/02/12/2016/584120739a794778590e2961
2. Колимечков Б. Российские банки готовы к кибератакам извне // Life.ru. 2016. URL: https://life.ru/t/%D0%B1%D0%B0%D0%BD%D0%BA%D0%B8/940692/rossiiskiie_banki_ghotovy_k_kibieratakam_izvnie
3. Ненашев С.М. Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей // Вопросы кибербезопасности. 2016. № 5 (18). С. 65-72.
4. Ненашев С.М. Прогнозирование реакции пользователей социальной сети «ВКонтакте» на публикации о субъектах экономики // Оборонный комплекс – научно-техническому прогрессу России. 2019. № 1 (141). С. 3-10.
5. Новиков Ю.И., Бандурко С.А. Социальные сети как фактор операционного риска банка // Известия Санкт-Петербургского государственного экономического университета. 2015. № 3 (93). С. 98-102.
6. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008. 320 с.
7. ФСБ России предупредила пользователей соцсетей и сотовых абонентов о возможных провокациях. URL: http://sakhaday.ru/news/fsb-rossii-predupredila-polzovatelej-sotssetej-i-sotovyh-abonentov-o-vozmozhnyh-provokatsiyah
8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «Форум», Инфра-М, 2009.
9. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. М.: Гелиос АРВ, 2005.
10. Miranda F.J., Chamorro A., Rubio S., Morgado V. Evaluation of Social Networks Sites in the Banking Sector: An Analysis of Top 200 International Banks // Journal of Internet Banking and Commerce. 2013. Vol. 18. No. 2.

Threats to information security of banks related to the use of social media

Sergei M. Nenashev

Postgraduate,
Financial University under the Government of the Russian Federation,
125993, 49 Leningradskii av., Moscow, Russian Federation;
e-mail: snenashev@gmail.com

Abstract

Social networks are a direct, fast and almost free channel of communication with customers, so the interest of Russian and foreign banks to them is constantly growing. The presence of banks in social networks creates specific threats to the information security of banks and their customers. The article discusses some of these threats and proposes ways to counter them. The author notes that the enterprises of the financial sector, traditionally making significant efforts to ensure their own information security, should take into account all possible security threats related to the use of social networks, in information security policy and in plans for the development of information infrastructure of the enterprise. In order to counteract social engineering directed against bank customers, it is necessary to inform customers about all possible threats, as well as to exclude social networks from the obvious channels of communication between employees allowed by the information security policy for the exchange of any information related to the bank's activities. The threats related to the collection of personal data of users of social networks who are clients of banks are primarily associated with the ability to establish with a significant degree of confidence that some person is a client of the bank upon subscription of a user of the social network to the official co-society of the bank in the social network. Therefore, it is necessary to close the list of subscribers

of official groups of banks from viewing by any users in social networks that provide such an opportunity.

For citation

Nenashev S.M. (2019) Ugrozy informatsionnoi bezopasnosti bankov, svyazannye s ispol'zovaniem sotsial'nykh setei [Threats to information security of banks related to the use of social media]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 9 (4A), pp. 17-23.

Keywords

Bank, threat to information security, customer, social media, communication channel, financial sector.

References

1. *FSB Rossii predupredila pol'zovatelei sotssetei i sotovykh abonentov o vozmozhnykh provokatsiyakh* [The Federal Security Service of the Russian Federation warned users of social networks and mobile subscribers about possible provocations]. Available at: http://sakhaday.ru/news/fsb-rossii-predupredila-polzovatelej-sotssetej-i-sotovyh-abonentov-o-vozmozhnyh-provokatsiyah [Accessed 18/04/19].
2. Kalyukov E. et al. (2016) FSB soobshchila o podgotovke inostrannymi spetssluzhbami kiberataki na banki [The Federal Security Service has reported on the preparation of cyber attacks on banks by by the foreign intelligence agencies]. *RBK*. Available at: http://www.rbc.ru/finances/02/12/2016/584120739a794778590e2961 [Accessed 16/04/19].
3. Kolimechkov B. (2016) Rossiiskie banki gotovy k kiberatakam izvne [Russian banks are ready to cyber attacks from outside]. *Life.ru*. Available at: https://life.ru/t/banki/940692/rossiiskiie_banki_ghotovy_k_kibieratakam_izvnie [Accessed 16/04/19].
4. Miranda F.J., Chamorro A., Rubio S., Morgado V. (2013) Evaluation of Social Networks Sites in the Banking Sector: An Analysis of Top 200 International Banks. *Journal of Internet Banking and Commerce*, 18 (2).
5. Nenashev S.M. (2016) Informatsionno-tekhnologicheskaya i informatsionno-psikhologicheskaya bezopasnost' pol'zovatelei sotsial'nykh setei [Information-technical and information-psychological security of social-network users]. *Voprosy kiberbezopasnosti* [Issues of cybersecurity], 5 (18), pp. 65-72.
6. Nenashev S.M. (2019) Prognozirovanie reaktsii pol'zovatelei sotsial'noi seti "VKontakte" na publikatsii o sub"ektakh ekonomiki [Prediction of the reaction of users of the social network "VKontakte" on the publication of the subjects of the economy]. *Oboronnyi kompleks – nauchno-tekhnicheskomu progressu Rossii* [Defense complex for scientific and technical progress of Russia], 1 (141), pp. 3-10.
7. Novikov Yu.I., Bandurko S.A. (2015) Sotsial'nye seti kak faktor operatsionnogo riska banka [Social networks as a factor of operational risk of the bank]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta* [Proceedings of St. Petersburg State University of Economics], 3 (93), pp. 98-102.
8. Shan'gin V.F. (2009) Informatsionnaya bezopasnost' komp'yuternykh sistem i setei [Information security of computer systems and networks]. Moscow: ID "Forum", Infra-M Publ.
9. Shumskii A.A., Shelupanov A.A. (2005) *Sistemnyi analiz v zashchite informatsii* [System analysis in information protection]. Moscow: Gelios ARV Publ.
10. Skiba V.Yu., Kurbatov V.A. (2008) *Rukovodstvo po zashchite ot vnutrennikh ugroz informatsionnoi bezopasnosti* [A guide to protection against internal threats to information security]. Saint Petersburg: Piter Publ.