некоммерческое партнерство
национальный платежный совет

АРСИБ
АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Угрозы ПДн в банковской системе «Страхи» и «Реалии»

Алексей Ермаченков
ermachenkov@promsberbank.ru
Член РГ по защите информации в НПС
КТН

Павел Головлев
pgolovlev@smpbank.ru
Член РГ по защите информации в НПС
Член АРСИБ

DISCLAIMER

Мнение, высказанное в настоящем докладе, является личным мнением авторов и может не совпадать ни с одной официальной позицией и даже быть ошибочным.

Все, о чем пойдет речь далее, имеет отношение ТОЛЬКО к вопросам защиты персональных данных.

Угрозам в системах ДБО, карточном и другом банковском бизнесе посвящены другие исследования.

п. 1.5 ст. 18.1 152-ФЗ: «оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;»

NB! Банковская система отличается от всех прочих тем, что объектом атаки в ней являются непосредственно денежные средства.

При этом атака осуществляется через использование ПДн, полученных из других систем.

При этом законодательно клиенты банков защищены как нигде более.

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)

Роскомнадзор получил необходимые для работы по защите прав субъектов персональных данных социологические выкладки

3 мая 2013 года

По результатам проведенных Фондом общественного мнения социологических исследований выяснилось, как население России относится к преступлениям с использованием чужих персональных данных.

Опираясь на голоса опрошенных, настаивающих на том, с какими из этих правонарушений государство должно бороться в первую очередь, Роскомнадзор составил своеобразный рейтинг.

На основании полученных результатов Служба намерена скорректировать свои подходы к реализации функций уполномоченного органа власти по защите прав субъектов персональных данных. *(http://www.rsoc.ru/news/rsoc/news19803.htm)*

61% голосов - незаконное использование паспортных данных для оформления кредита, ипотеки и т.д.

- ✓ Ущерб для клиента: 0

- ✓ Ущерб для банка: невозврат кредита, резервы, судебные издержки

61% - мошенничество с кредитными картами;

- ✓ Ущерб для клиента: средний остаток на карточном счете в разрезе карты, если доказана вина.
- ✓ Ущерб для банка: средний остаток на карточном счете в разрезе клиентской базы, судебные издержки, санкции со стороны МПС.

27% - мошенничество с электронными деньгами, СМС-оплатой;

- ✓ Ущерб для клиента: 0

- ✓ Ущерб для банка: 0

Указанные данные в банковских системах не обрабатываются.

23% - использование персональных данных для осуществления рассылки рекламных сообщений (спам) на мобильный телефон или электронную почту;

- ✓ Ущерб для клиента: ~0

- ✓ Ущерб для банка: штрафные санкции, репутационные и иные издержки

20% - телефонные звонки с предложением товаров и услуг;

- ✓ Ущерб для клиента: ~0

- ✓ Ущерб для банка: штрафные санкции, репутационные и иные издержки

17% - публикация персданных в СМИ без разрешения владельца;

- ✓ Ущерб для клиента: моральный вред (???)

- ✓ Ущерб для банка: нарушение банковской тайны, штрафные санкции, репутационные и иные издержки.

17% - взлом социальных сетей и распространение персональной информации (номер телефона, адрес и т.д.);

- ✓ Ущерб для клиента: моральный вред (???)

- ✓ Ущерб для банка: 0

Указанные данные в банковских системах не обрабатываются.

15% - публикация персональных данных в интернете без разрешения владельца;

- ✓ Ущерб для клиента: моральный вред (???)
- ✓ Ущерб для банка: нарушение банковской тайны, штрафные санкции, репутационные и иные издержки.

п. 1.5 ст. 18.1 152-ФЗ: «оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;»

7% - пожалуются в РКН в случае получения третьими лицами кредитов по их паспортным данным;

7% - при любых возможных материальных потерях, возникших с использованием их персданных;

5% - готовы прибегнуть к помощи уполномоченного органа в случае любого мошенничества;

3% - придут в Роскомнадзор только из-за конкретных манипуляций с банковскими картами и счетами.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также **с учетом экономической целесообразности** на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от "14" мая 2013.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818),

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

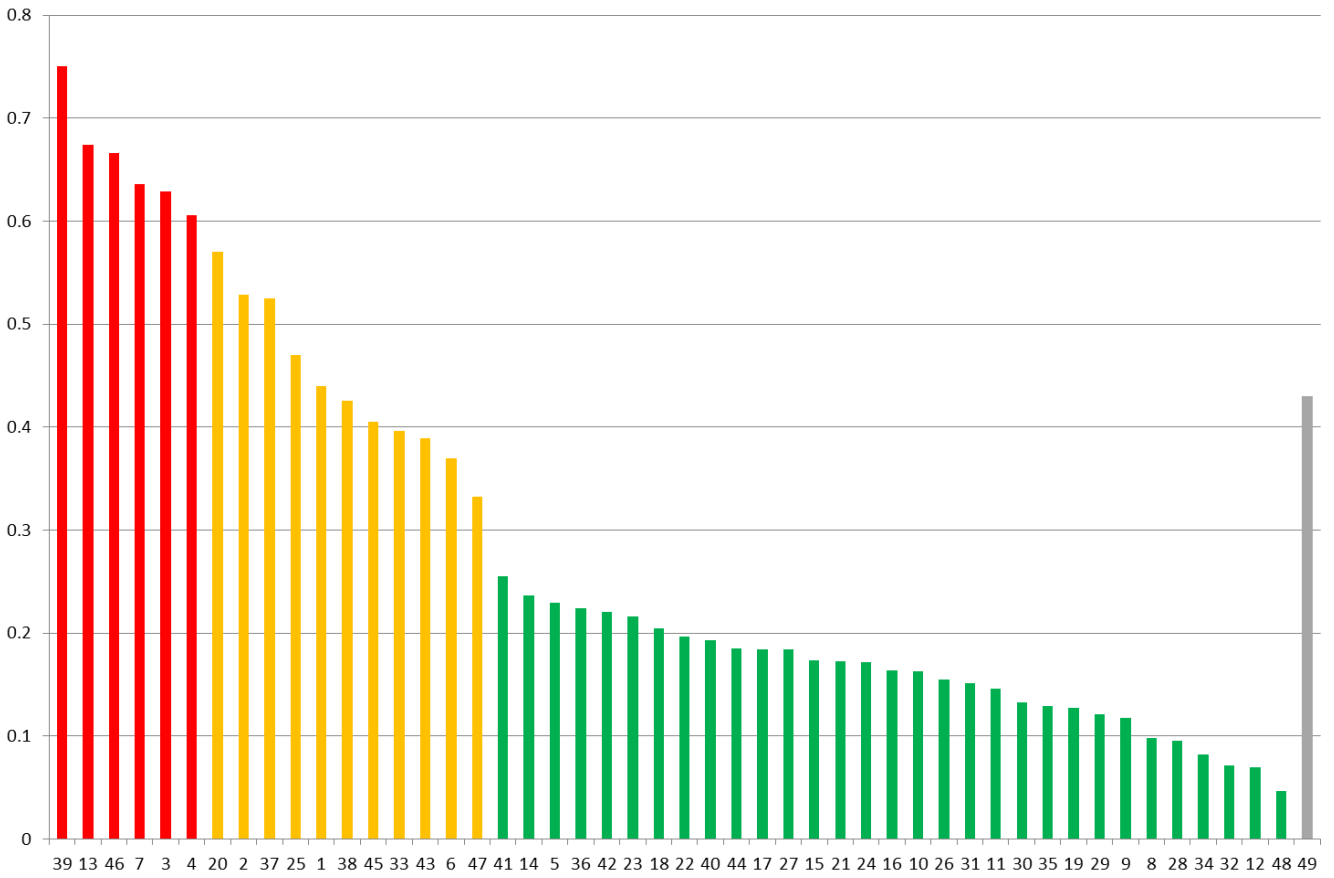
Таким образом, в банковской системе реализация любой угрозы приводит исключительно к незначительным негативным последствиям для субъектов персональных данных и имеет «низкий» показатель опасности угрозы.

Любая информационная система банка имеет уровень защищенности выше или равный «низкому» и вероятность реализации угрозы ниже или равную «средней».

В соответствии с Методикой определения актуальных угроз безопасности персональных данных, утвержденной ФСТЭК 14.02.2008, возможность реализации угроз в любой информационной банковской системе будет не выше «высокой» *(Y=0.75)*.

Рабочая группа АРБ и НПС в составе экспертов из 35 банков, совокупные активы которых составляют более 22.8 трлн.руб., под эгидой ГУБЗИ ЦБ составила список из 48 угроз персональным данным при их обработке в информационных банковских системах.

Из них имеют высокую возможность реализации угрозы и, соответственно, являются актуальными 6:



39) Осуществление несанкционированного доступа к персональным данным путем использования методов социального инжиниринга к легальным субъектам доступа.

13) Осуществление несанкционированного доступа к персональным данным с использованием уязвимостей, вызванных недостатками организации защиты персональных данных.

46) Осуществление несанкционированного доступа к персональным данным путем внедрения вредоносного программного обеспечения.

7) Утрата (потеря) накопителей с персональными данными, включая переносные персональные компьютеры пользователей информационной системы персональных данных.

3) Использование системного и прикладного программного обеспечения автоматизированных рабочих мест пользователей информационной системы персональных данных, приводящее к несанкционированному доступу к персональным данным.

4) Осуществление несанкционированного доступа к персональным данным в ходе сопровождения, модернизации и (или) вывода из эксплуатации компонентов информационной системы персональных данных.

некоммерческое партнерство
национальный платежный совет

АРСИБ
АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Поправьте меня, если я не прав!

Павел Головлев
paulmg69@gmail.com

Член комитета по банковской безопасности АРБ
Член РГ по разработке Стандартов, Указаний и Рекомендаций по защите информации в НПС
Член АРСИБ