Дистанционное банковское обслуживание - взгляд клиента

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Ермаченков А.В., ктн

Причина

В холдинге используются 9+ ДБО от различных банков.

Требования ИБ для ДБО включаются:

- **договор (раздел клиент обязан);**
- **приложение к договору;**
- **ссылку в договоре на документ на сайте банка;**
- **труднонаходимые рекомендации на сайте банка.**

Даже рекомендации, в случае их невыполнения, могут сыграть свою негативную роль в случае фрода. Банк на это будет опираться при своей защите.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Противоречия?

Исключайте посещение с ПК, на которых осуществляется подготовка и отправка документов в Банк, сайтов сомнительного содержания и любых других Интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п.), чтение почты и открытие почтовых вложений от недоверенных источников, установку и обновление любого ПО не с сайтов производителей. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивайте «белым списком» со всех рабочих мест, на которых осуществляется подготовка, подписание и отправка платежных документов. В «белый список» должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в производственном процессе, сервера обновлений системного и антивирусного ПО.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

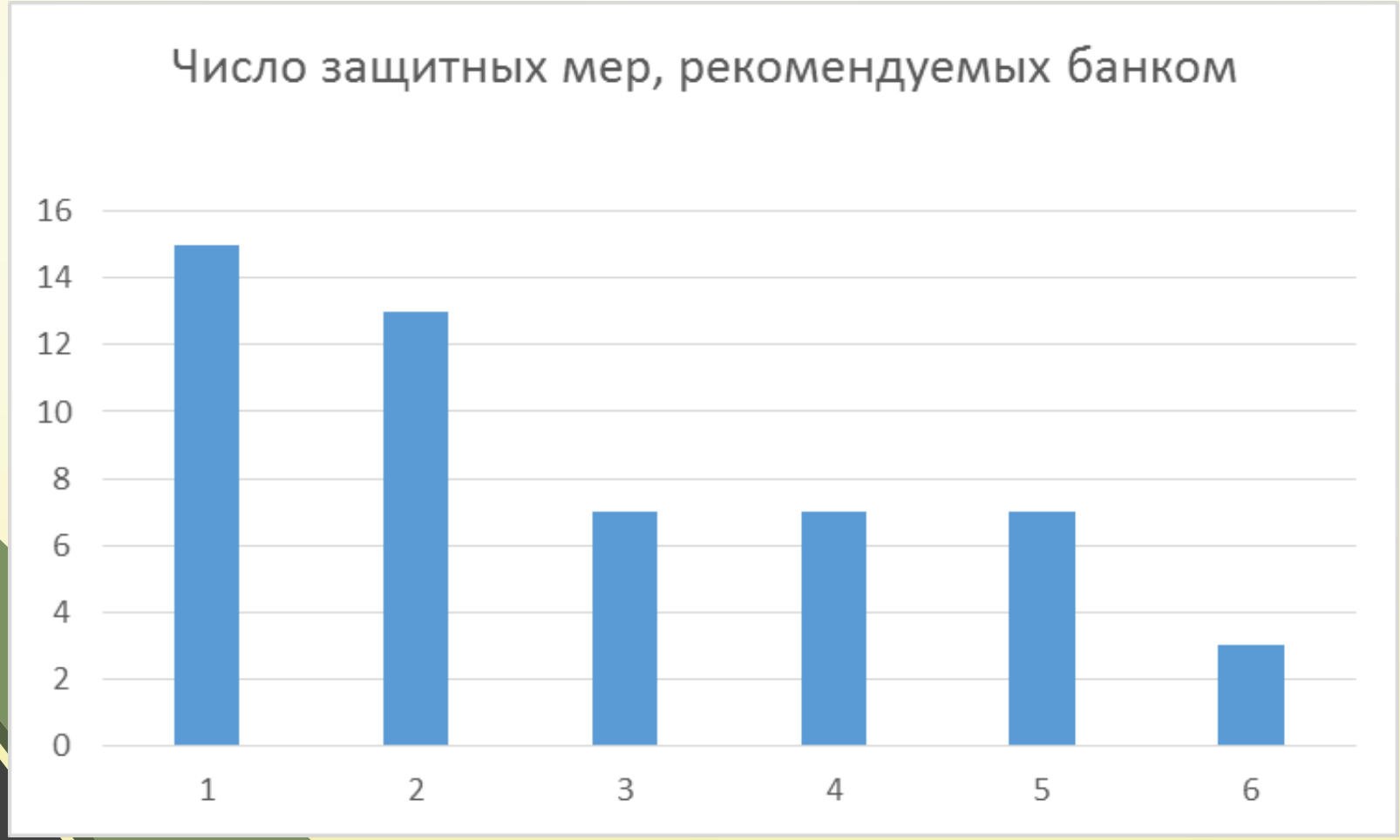
Анализ требований

Всего выделено 23 требования.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Анализ банков

На примере 6 банков.



ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Следствие:

Защитная мера:

Разработка и распространение материалов (мультимедиа, брошюры, плакаты, заставки и т.д.), повышающих бдительность клиентов.

Снижает для банка потери от фрода на 12%.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Следствие:

При первом аудите зафиксировано выполнение 25% технических требований.

После проведения корректирующих работ, исполняются 100% технических требований. В том числе:

1. Регулярное проведение антивирусной проверки на компьютерах.

2. Запрет на использование программ удаленного управления компьютером.

3. Доступ в Интернет по «белому» списку сайтов.

4. Ограничен сетевой доступ к компьютерам.

5. Не использовать учетные записями, имеющими административные права.

6. Минимизировать количество пользователей компьютеров.

7. Установить надёжные пароли на вход в компьютер, обеспечить периодическую смену этих паролей.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Пример 1.

https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Pamjatka_Upravlenie_K_preduprezhdaet

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН-КОД КАРТЫ
2. ВЫУЧИТЬ ПИН-КОД ЛИБО ХРАНИТЬ ЕГО ОТДЕЛЬНО ОТ КАРТЫ И НЕ В БУМАЖНИКЕ
3. НЕ ПЕРЕДАВАТЬ КАРТУ ДРУГИМ ЛИЦАМ – ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ
4. ПОЛЬЗОВАТЬСЯ ТОЛЬКО БАНКОМАТАМИ НЕ ОБОРУДОВАННЫМИ ДОПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ
5. ПО ВСЕМ ВОПРОСАМ СОВЕТОВАТЬСЯ С БАНКОМ, ВЫДАВШИМ КАРТУ

Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты Управления «К» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

Министерство внутренних дел Российской Федерации

Управление «К» МВД РФ предупреждает!

ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ

Будьте осторожны и внимательны!

Мошенничества с пластиковыми картами

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Пример 2.

http://arb.ru/b2b/docs/metodicheskie_rekomendatsii_o_poryadke_deystviy_v_sluchae_vyyavleniya_khishcheni-1699733/

Ассоциация Российских Банков

ПРО БАНКИ › ДОКУМЕНТЫ

Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента

Настоящие рекомендации разработаны Рабочей группой Ассоциации российских банков и НП «Национальный платежный совет» по предотвращению мошенничества в платежных системах (далее – Рабочая группа) с учетом Письма Бюро специальных технических мероприятий Министерства внутренних дел Российской Федерации (далее – БСТМ МВД России) от 17 января 2012 г. № 10/257 с целью разъяснения порядка действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания (далее – ДБО), использующих электронные устройства (далее – ЭУ): персональный компьютер, ноутбук, планшетный компьютер и т.п. в качестве удаленного рабочего места для целей дистанционного управления денежными средствами клиента.

Прикрепленные документы

Полный текст документа (doc, 245 Kb)

ГРУППА КОМПАНИЙ МОСПРОЕКТ-3

Предложения

В договор:

1. Обеспечивать конфиденциальность ключей ЭЦП, не допускать не санкционированного использования ключей.
2. Использование современного антивирусного обеспечения. Регулярное обновление антивирусного программного обеспечения.
3. Регулярное проведение антивирусной проверки на компьютерах.
4. Своевременная установка обновлений **безопасности** операционной системы **и программного обеспечения** компьютеров.
6. Настройки сетевого оборудования, корпоративных и персональных сетевых экранов выход в Интернет должен быть ограничен «белым списком» доверенных сайтов.
8. Не работать на компьютерах, на которых осуществляется подготовка и отправка документов в Банк, под учетными записями, имеющими административные права.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Предложения

9. Минимизировать количество пользователей компьютеров, на которых осуществляется подготовка и отправка документов в Банк.
10. Установить надёжные пароли на вход в компьютер, обеспечить периодическую смену этих паролей.
11. Поддерживать точность системного времени компьютера по местному времени с точностью **до 1 минуты**.
12. Ограничить физический доступ к компьютерам, на которых осуществляется подготовка и отправка документов в Банк, допускаются только работники, непосредственно уполномоченные на работу с программным обеспечением «Интернет Банк-Клиент».
13. Хранить ключевые носители **способом**, исключающем несанкционированный доступ к ним.

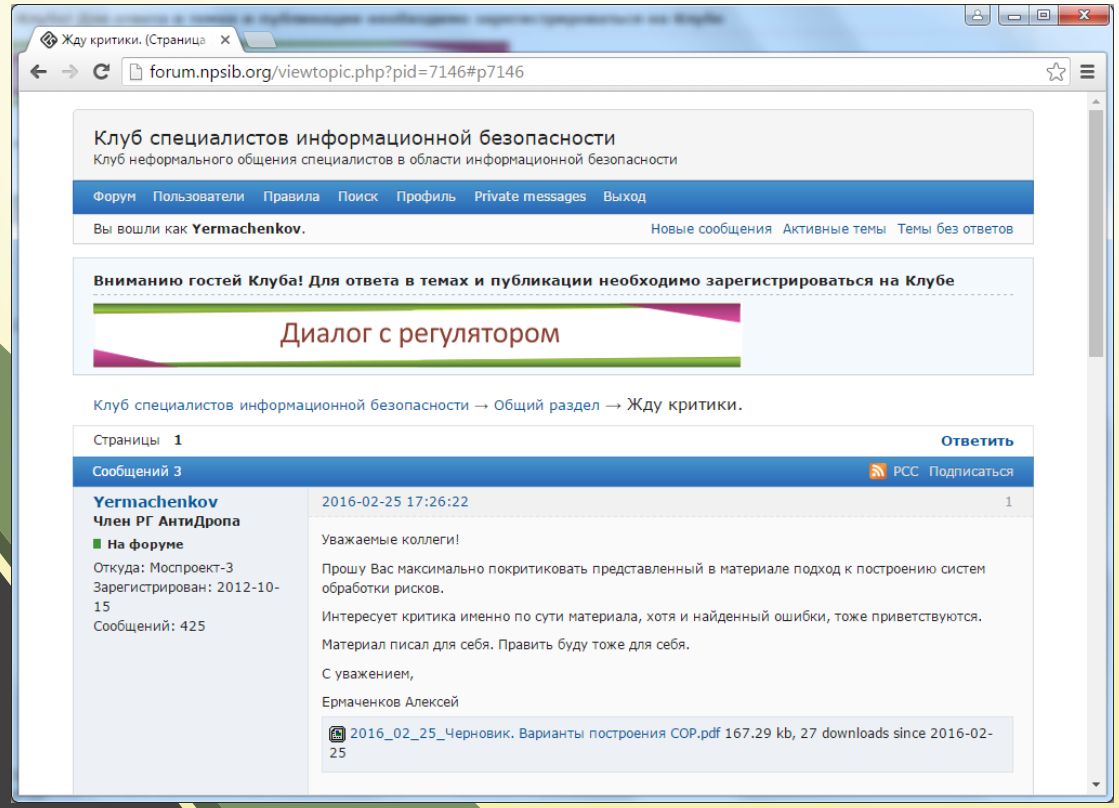
14. Оргмеры обязательные:
a. Самостоятельно генерировать секретный ключ;
b. Регулярно контролируйте состояние своих счетов;
c. Не передавать пароли к секретным ключам, не записывать и не сохранять пароли вместе с носителем ключа.

ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Спасибо за внимание…

Приглашаю покритиковать:

http://forum.npsib.org/viewtopic.php?pid=7146#p7146



ГРУППА КОМПАНИЙ
МОСПРОЕКТ-3

Ермаченков А.В., ктн