Банк России
Центральный банк Российской Федерации

FinCERT – первые результаты

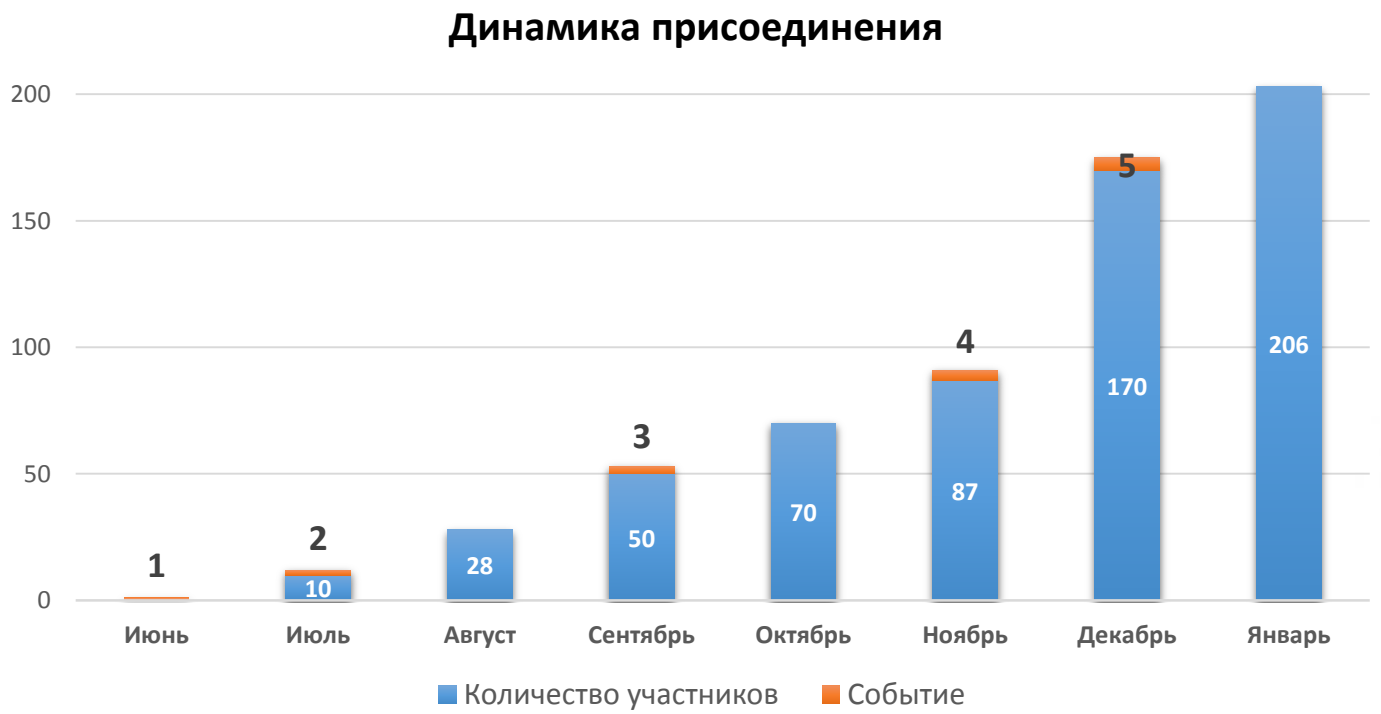
Сударенко Артем
ГУБиЗИ Банка России

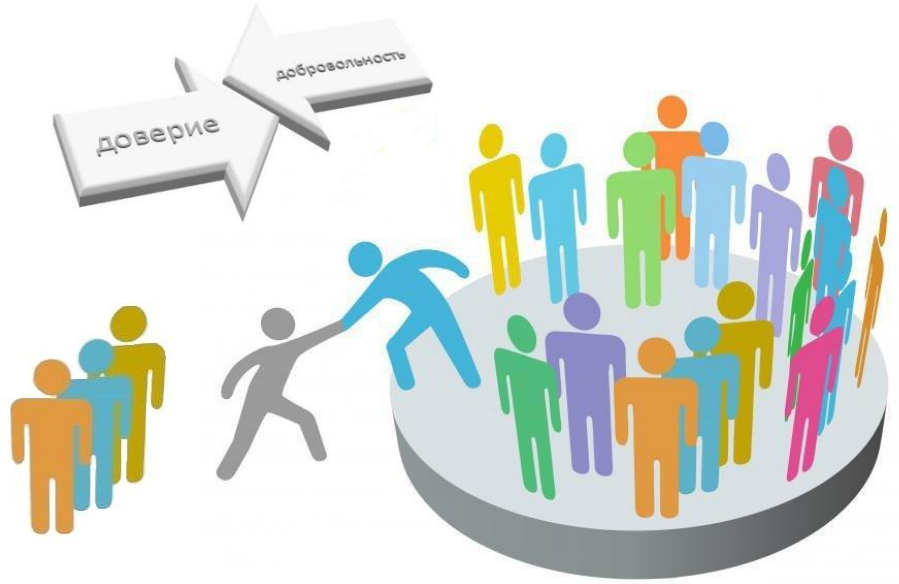
Присоединение кредитных организаций к информационному обмену

Присоединение кредитных организаций к информационному обмену

Присоединение кредитных организаций к информационному обмену

Присоединение кредитных организаций к информационному обмену





1. Начало работы;

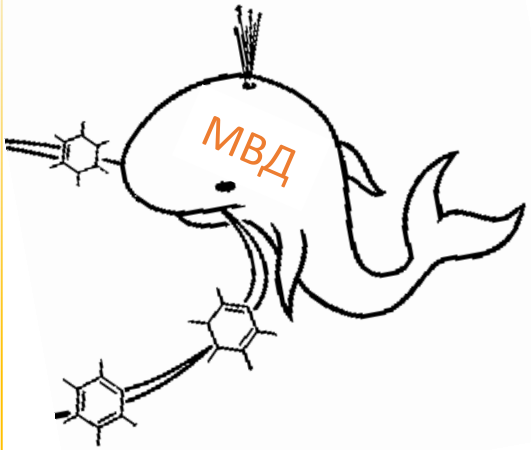
2. Выступление на заседании в АРБ;

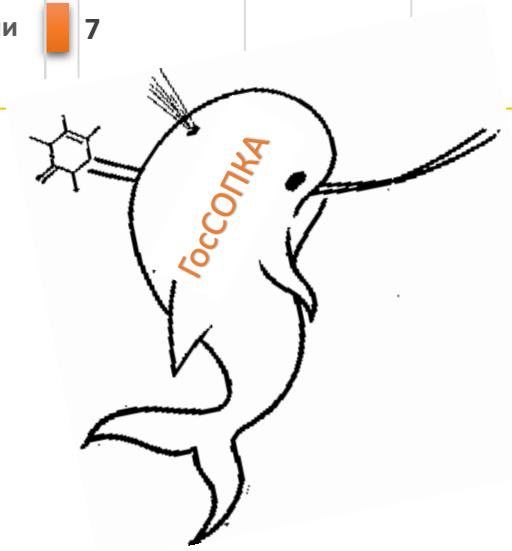
3. ***Рассылка*** в рамках «клуба Антидроп»;

4. ***Рассылка*** через ГУ ЦБ РФ;

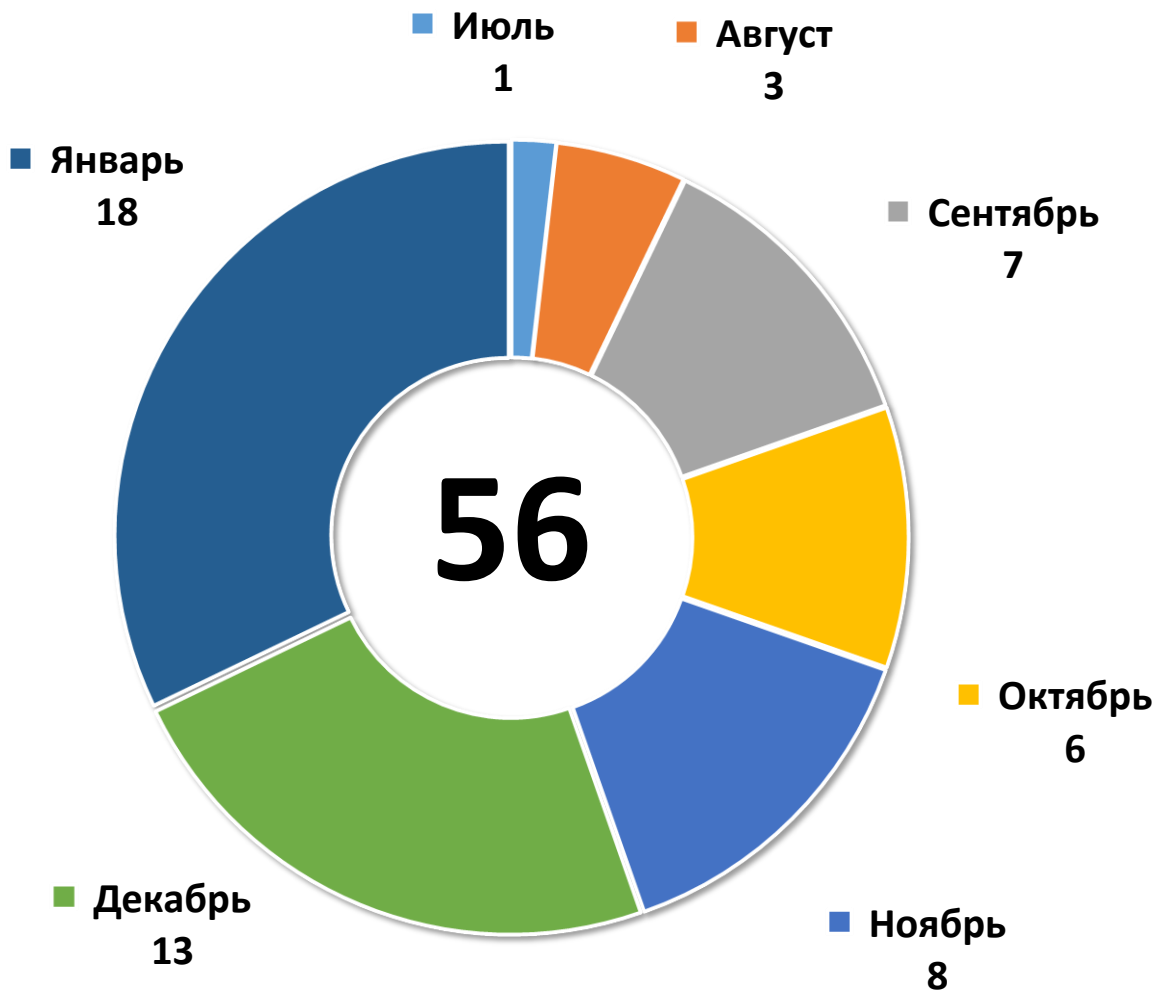
5. Всего ***203 КО*** по состоянию на 15.02.2016.

Состав участников информационного обмена

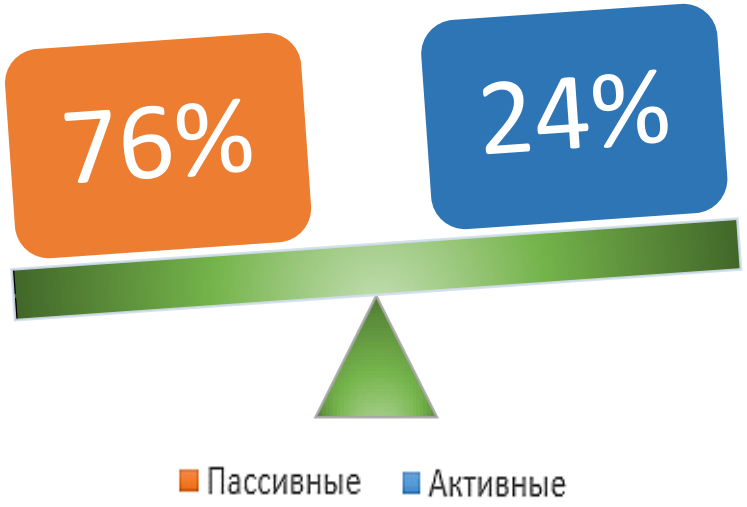




Оповещение участников информационного обмена



Вовлеченность участников в информационный обмен



Формат уведомлений в рамках информационного обмена

Уязвимости

ИР-20160122-003	**Уязвимость повышения привилегий в ядре Linux**
Описание уязвимости	Позволяет локальному пользователю получить административный доступ и скомпрометировать систему. Эксплуатация ошибки позволяет атакующему удалять файлы, просматривать конфиденциальную информацию, устанавливать нежелательные программы и пр.
Операционная система / аппаратная платформа	ОС Linux, ОС Android
Версия	версии ядра Linux от 3.8
Дата выявления / публикации	19.01.2016
Возможные меры по устранению уязвимости	На Linux-серверах эксплойт могут предотвратить такие средства защиты, как SMEP (Supervisor Mode Execution Protection) и SMAP (Supervicor Mode Access Protection), на Android-устройствах такую же функцию выполняет SELinux .
Статус уязвимости	Подтверждена Perception Point
Наличие эксплойта	Есть
Информация об устранении	Уязвимость устраняется
Ссылки на источники	https://threatpost.ru/serious-linux-kernel-vulnerability-patched/14275/
Идентификаторы других систем описания уязвимостей	CVE-2016-0728
Прочая информация	Отсутствует

Формат уведомлений в рамках информационного обмена

Угрозы

FinCERT Банка России

ВК-20160203-002

Рассылка информации о вредоносном коде Trojan.Crypt

1. Краткое описание угрозы

Рассылка писем, содержащая вирус-шифровальщик Trojan.Crypt. Тематика писем – информация по переводам.

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	-
2	Добавление отправителя в спам-фильтр на почтовом шлюзе	Почтовый адрес представлен в пункте 4
3	Блокировка задействованных адресов	Смотрите подпункт 4

3. Маркеры заражения (рассмотрены на одном из типов вредоносного вложения)

1. Вредоносный код представляет собой файл *030216scan.scr*. Относится к типу Trojan.Crypt. При активации происходит шифрование файлов и на компьютере появляется файл README, содержащий инструкции злоумышленников по осуществлению расшифровки. В частности, для связи предлагается использовать почтовый ящик **files2549@gmail.com**.

2. Маркеры вредоносного файла:

MD5:	82c9a56830474175168086abc08ffa08
SHA1	946a248bbfeee1087c9ea7cebfca149107d2d36c
SHA256	19c0eb5549e25a19394912d3759b5c2ba56b436b99453f2a35bc272a99137091

3. На 03.02.2016 вредоносный код детектируется следующими антивирусными решениями:
   - AegisLab
   - Bkav
   - ByteHero
   - Kaspersky
   - McAfee-GW-Edition

Email: fincert@cbr.ru

FinCERT Банка России

   - Qihoo-360

Ссылка:
https://www.virustotal.com/ru/file/19c0eb5549e25a19394912d3759b5c2ba56b436b99453f2a35bc272a99137091/analysis/

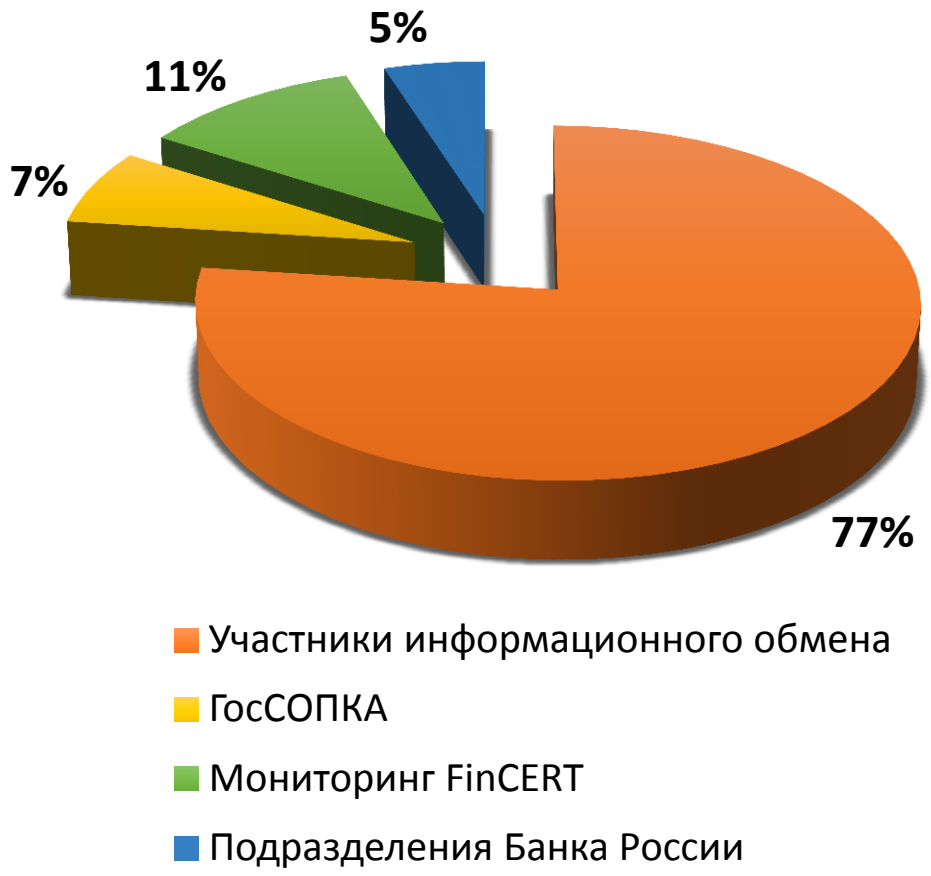
4. Сетевая активность: не зафиксирована.

4. Сведения об отправителе

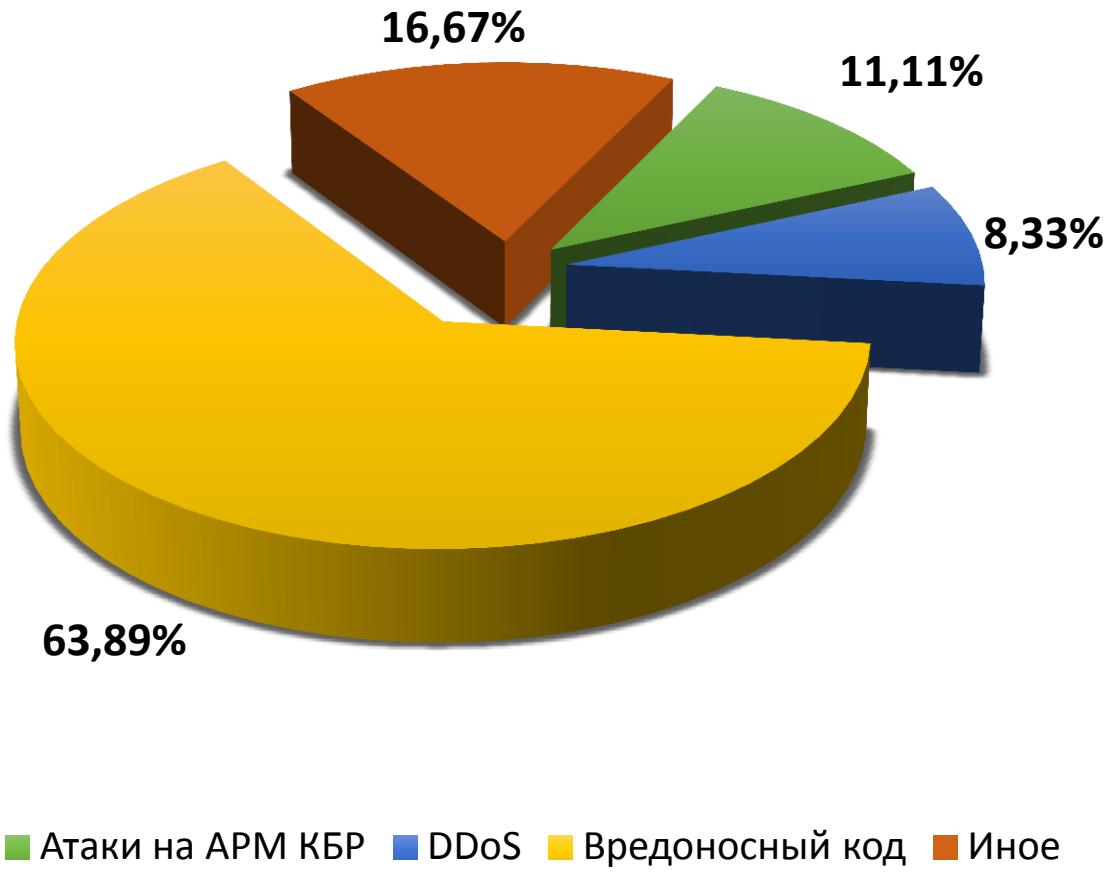
Отправитель (адрес)	**liulei16@126.com**
Текст письма	**Тема:** 5679oplata **Дата:** Wed, 3 Feb 2016 15:18:26 +0700 **От:** liulei16 Здравствуйте! Получен непонятный ваш перевод. В приложениэ детали платежа.

В случаях выявления заражения, просьба незамедлительно направлять информацию на электронный адрес fincert@cbr.ru, архив с паролем (например, *.rar), с указанием предполагаемого способа заражения.

Основные источники данных об атаках



Основные типы выявленных атак



Пример атаки на АРМ КБР

Пример атаки на АРМ КБР

Пример атаки на АРМ КБР

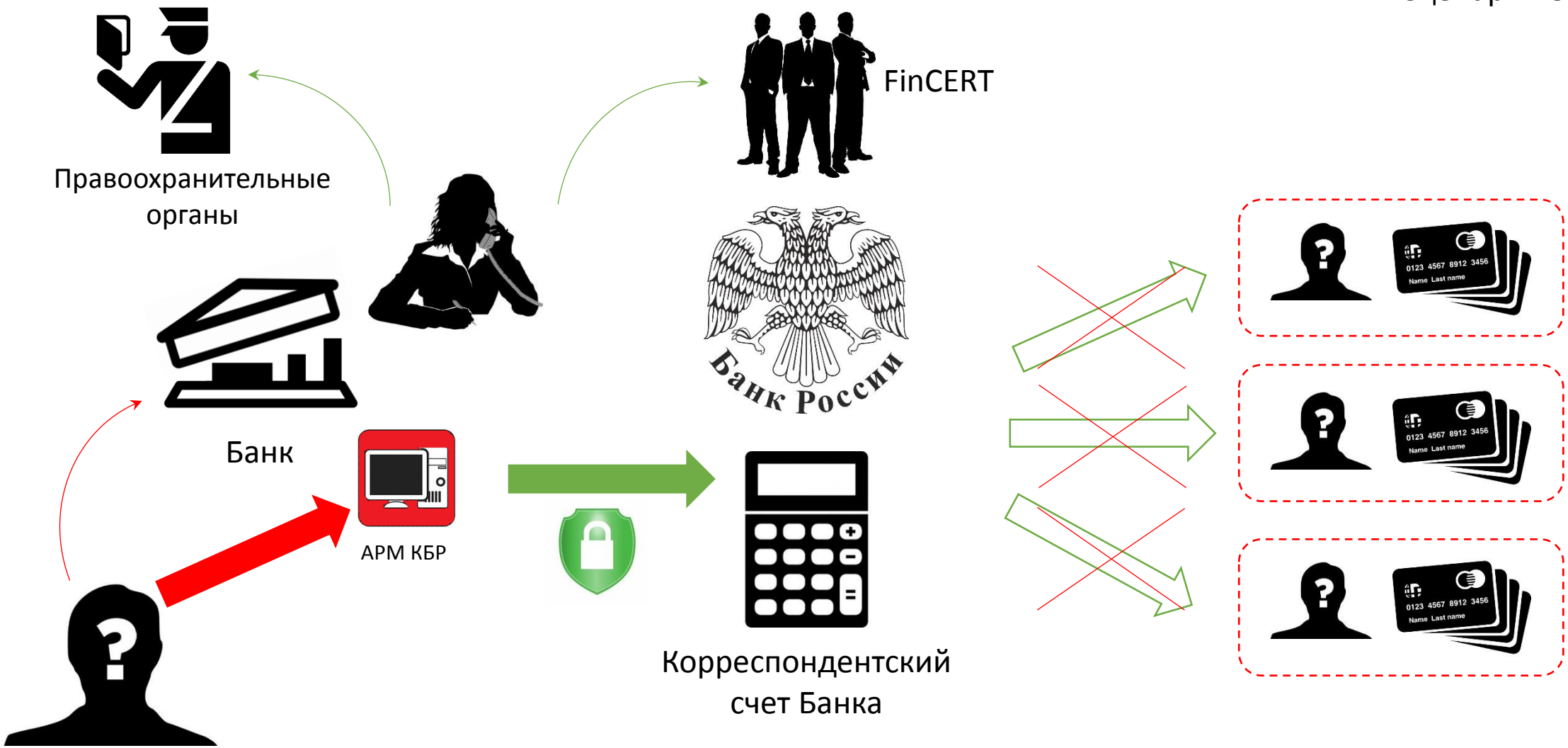
Сценарий 1

Пример атаки на АРМ КБР

Сценарий 2

Пример атаки на АРМ КБР

Сценарий 3



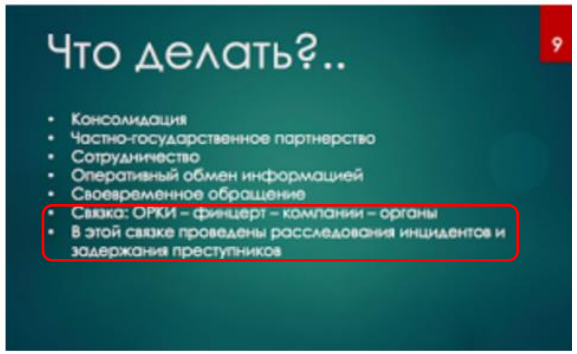
О нас говорят #FinCERT

17 Ноября, 2015

FinCERT: с чем его едят?

Алексей Лукацкий

Вот так выглядит на сегодня FinCERT. С прошедшего в феврале Уральского форума (а регистрация на новый уже открыта) видно движение вперед. Как в части налаживания работы самого центра и обеспечения его некоторой открытости (то, чего так не хватает ГосСОПКЕ), так и в части реальных результатов, о которых на SOC Forum говорил Руслан Стоянов из Лаборатории Касперского (есть реальные задержания киберпреступников).



Яндекс

fincert — 12 тыс. ответов

Найти

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Information Security №4/2015, 09 сентября 2015

BIS JOURNAL
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

BIS Journal №4(19)/2015, 5 ноября 2015


banki.ru

НОВОСТИ | БАНКИ И КОМПАНИИ | ПРОДУКТЫ И УСЛУГИ | РЕЙТИНГИ

FinCERT Банка России

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) – структурное подразделение главного управления безопасности и защиты информации Банка России (ГУБиЗИ).

FinCERT осуществляет сбор информации от финансовых учреждений о кибератаках, анализирует полученные сведения и дает обратную связь кредитно-финансовым организациям о возможных угрозах информационной безопасности, разрабатывает рекомендации по отражению хакерских атак, взаимодействует с правоохранительными органами и оперативными службами ФСБ. Также одной из основных задач центра является минимизация несанкционированных списаний с карт граждан. По данным Банка России, киберпреступники в 2014 году пытались вывести с банковских счетов 6 млрд рублей.

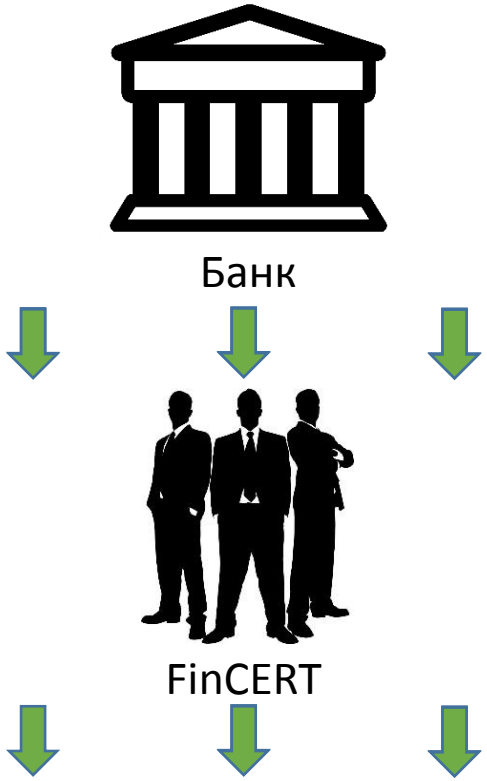
На сегодняшний день обязательных условий по предоставлению информации банками в центр нет, ее передача будет происходить на добровольной основе в свободном формате. Возможно, со временем передача финорганизациями сведений будет формализована.

Важно отметить, что, согласно указанию Банка России № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», банки с лета 2012 года уже предоставляют регулятору ежемесячно сведения о выявленных инцидентах при осуществлении перевода денежных средств, в частности в виде кражи (в том числе несостоявшейся).

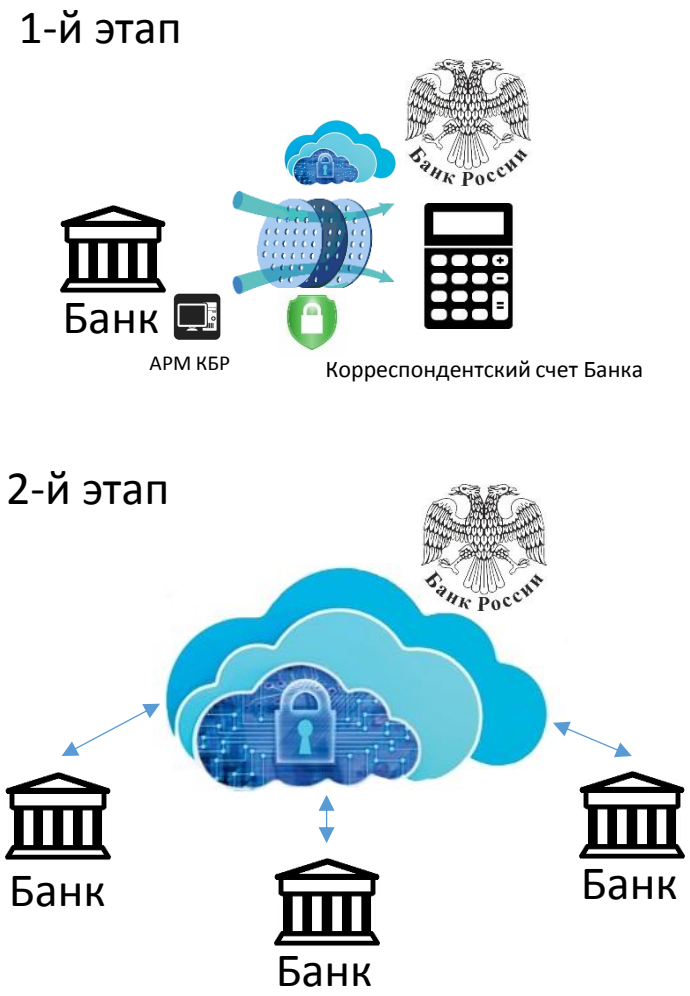
Центр начал свою работу 1 июня 2015 года, его возглавил начальник управления ГУБиЗИ Центробанка Дмитрий Фролов.

Перспективные направления

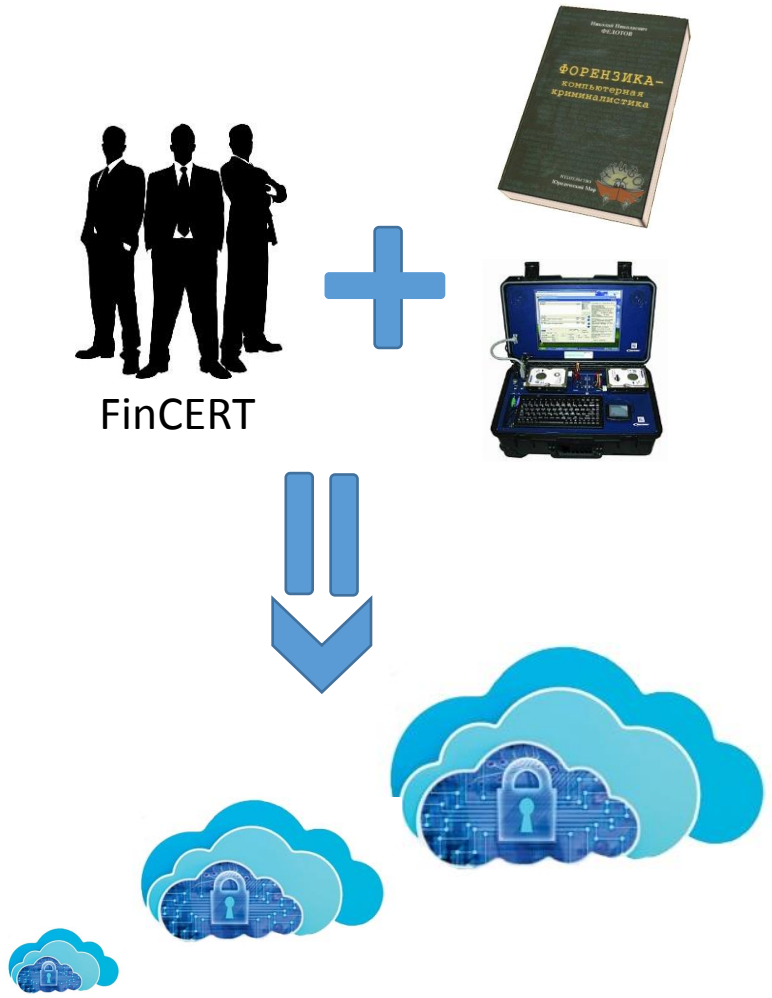
Антифишинг & Антиспам



Антифрод



Усиление технической экспертизы



Банк России
Центральный банк Российской Федерации

Спасибо за внимание!

Сударенко Артем

(Консультант FinCERT)

E-mail : sudarenkoaa@cbr.ru **FinCERT@cbr.ru**

Тел.: +7 (495) 771-99-99 (15598)