



Банк России

Центральный банк Российской Федерации



FinCERT: основные направления деятельности и результаты работы за год

Д.Б. Фролов
FinCERT Банка России

Основные принципы деятельности FinCERT



Добровольность



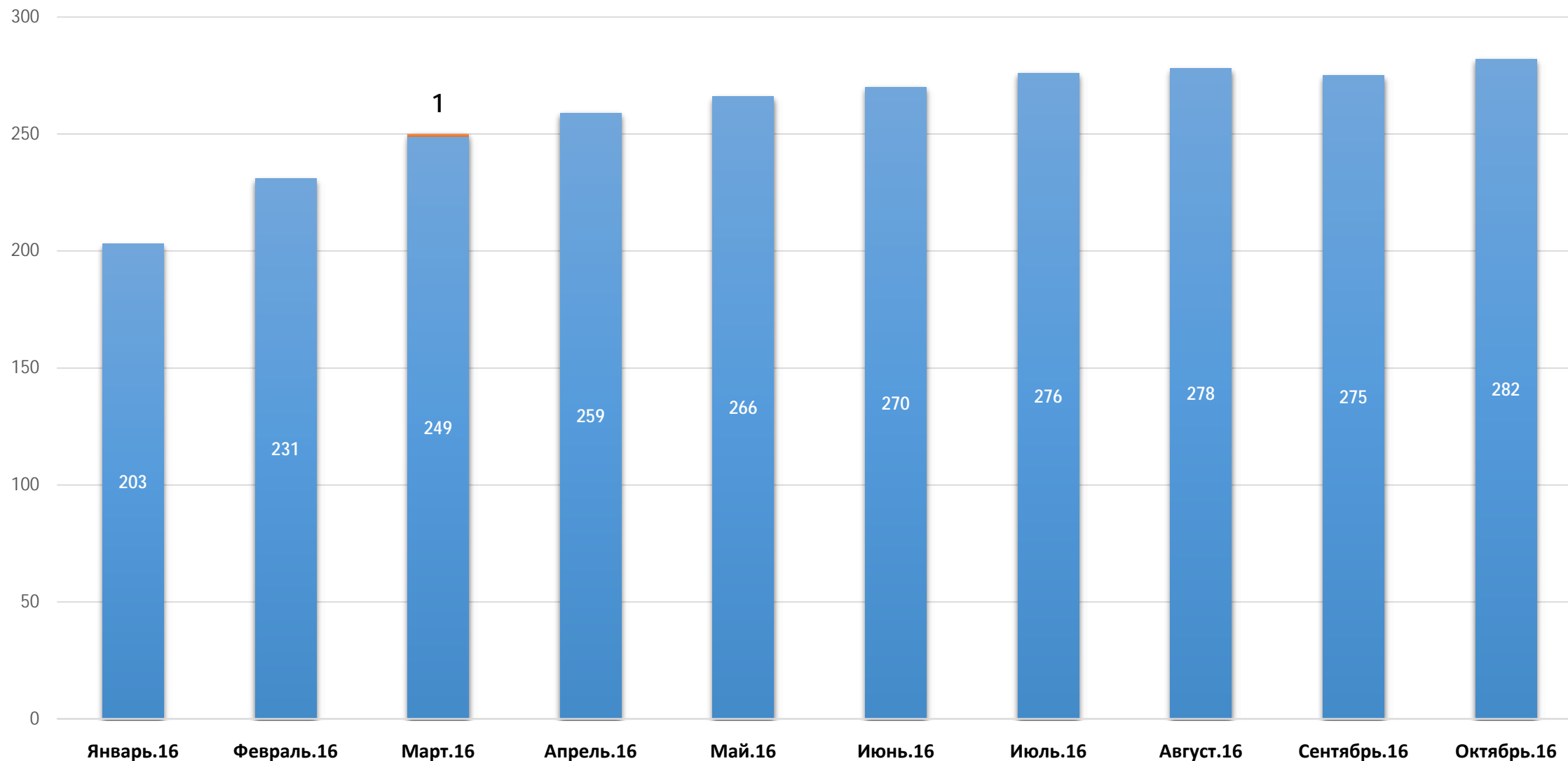
Открытость



Доверие



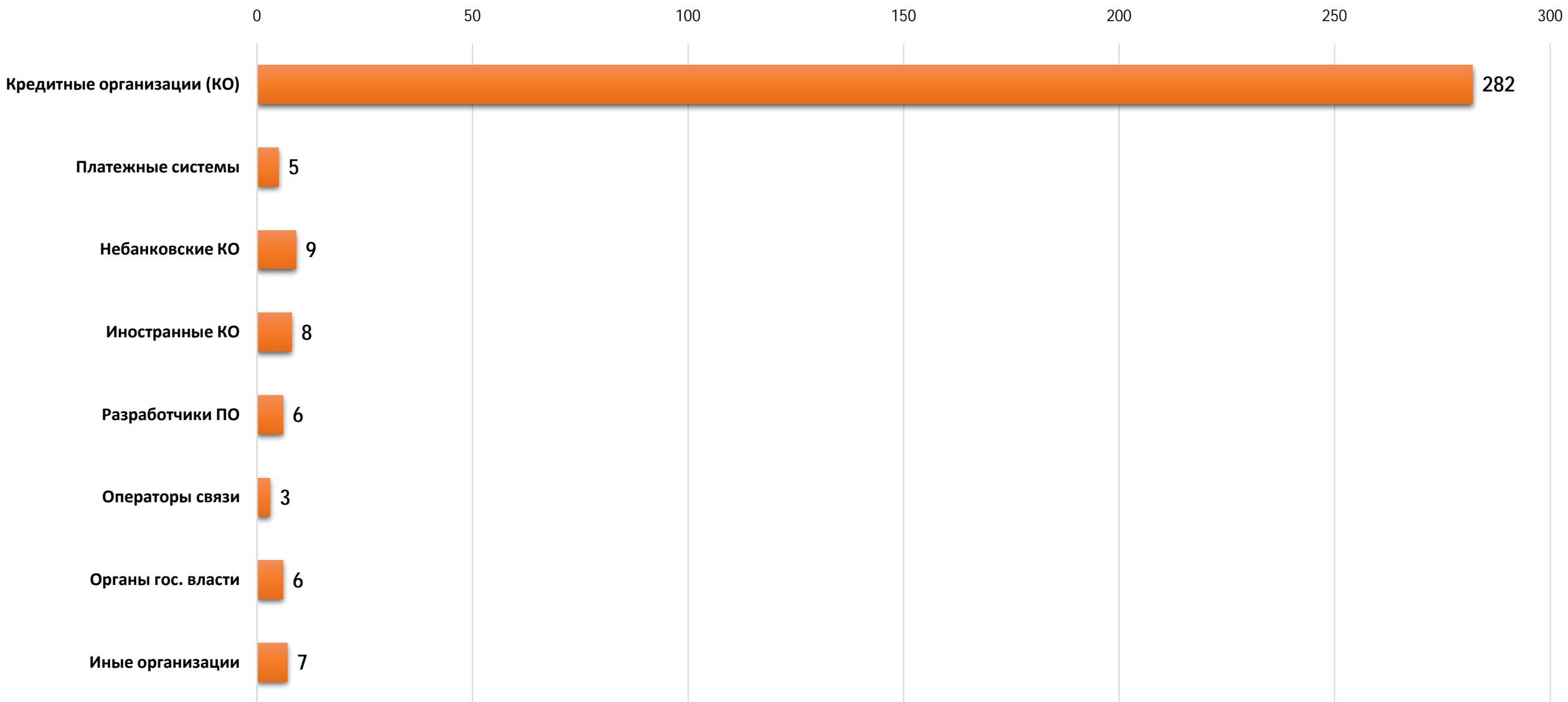
Динамика присоединения кредитных организаций к информационному обмену



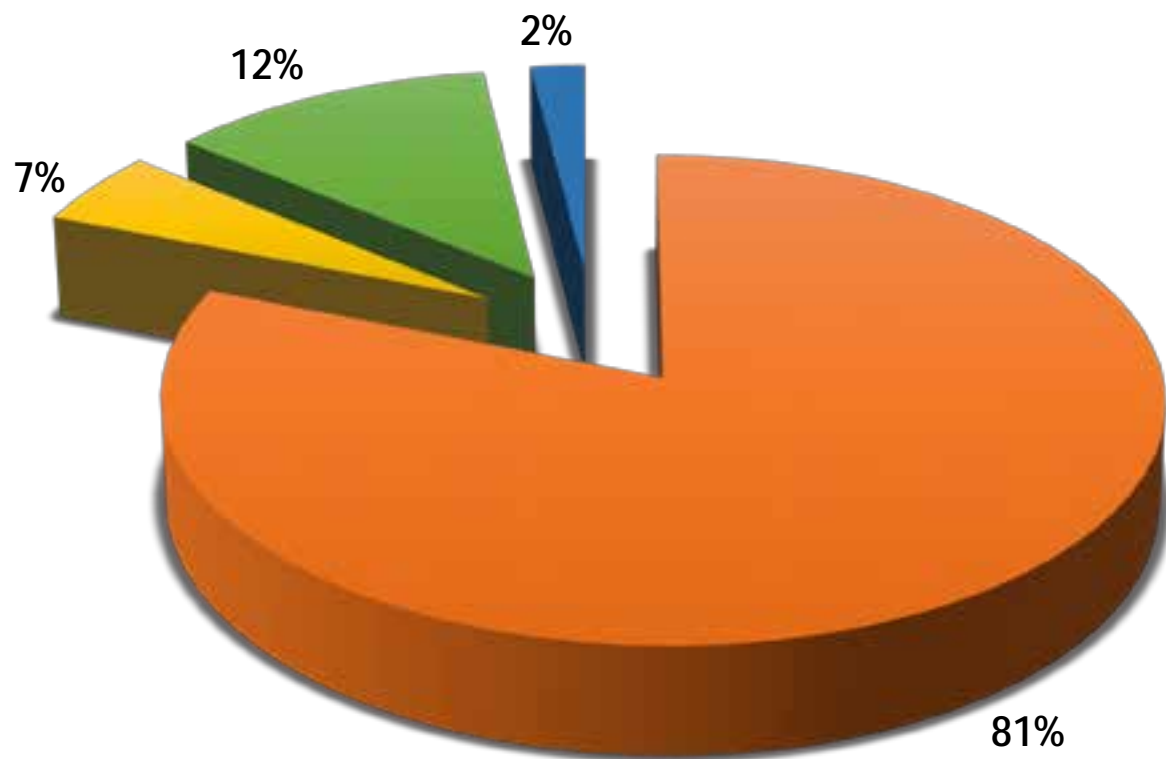
1. Рассылка писем от *fincer.net*.



Состав участников информационного обмена



Основные источники данных об атаках



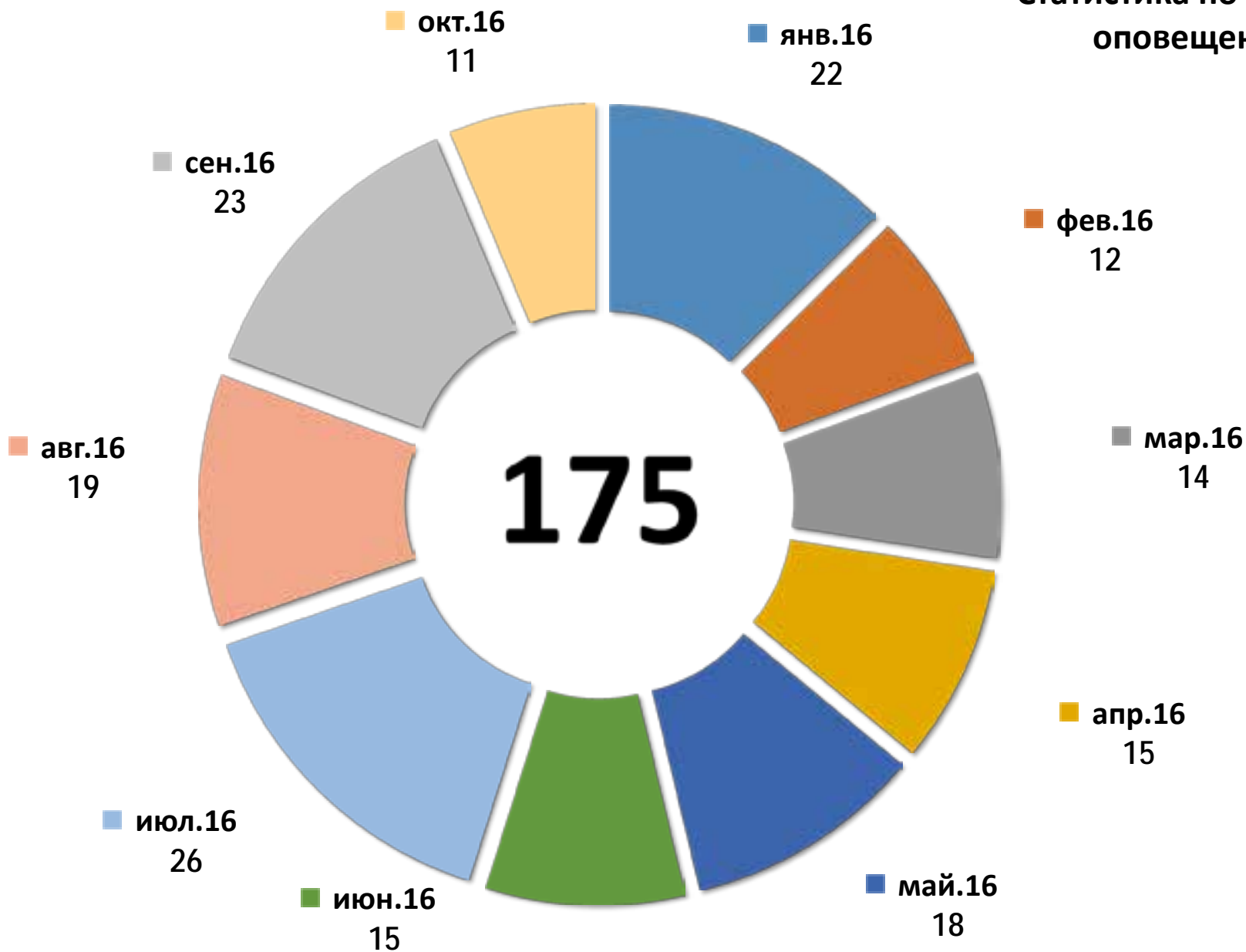
- Участники информационного обмена
- Правоохранительные органы + ГосСОПКА
- Мониторинг FinCERT
- Подразделения Банка России

Получена информация:

- 1 О распространении вредоносного ПО с использованием электронной почты и СМС;
- 2 О DDoS-атаках, направленных на внешние платежные сервисы и сайты КО;
- 3 О массовых СМС-рассылках от имени Банка России, платежных систем и КО;
- 4 Об атаках на банкоматы КО с использованием BlackBox;
- 5 О мошеннических действиях, с номеров в коде 8-800;
- 6 О доменах и почтовых адресах, участвующих в распространении вредоносного ПО, спама и фишинге.



Статистика по информационному оповещению участников





21 атака на платежные сегменты КО

~2,87 млрд. руб. пытались похитить

~1,2 млрд. руб. удалось вывести



Банк

Хищения через АРМ КБР



возбуждено **12** уголовных дел

~1,1 млрд. руб. временно заблокировано на счетах КО

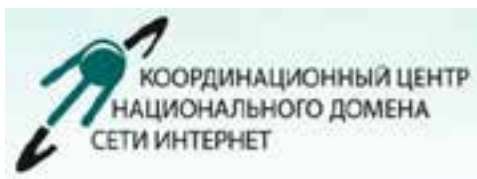
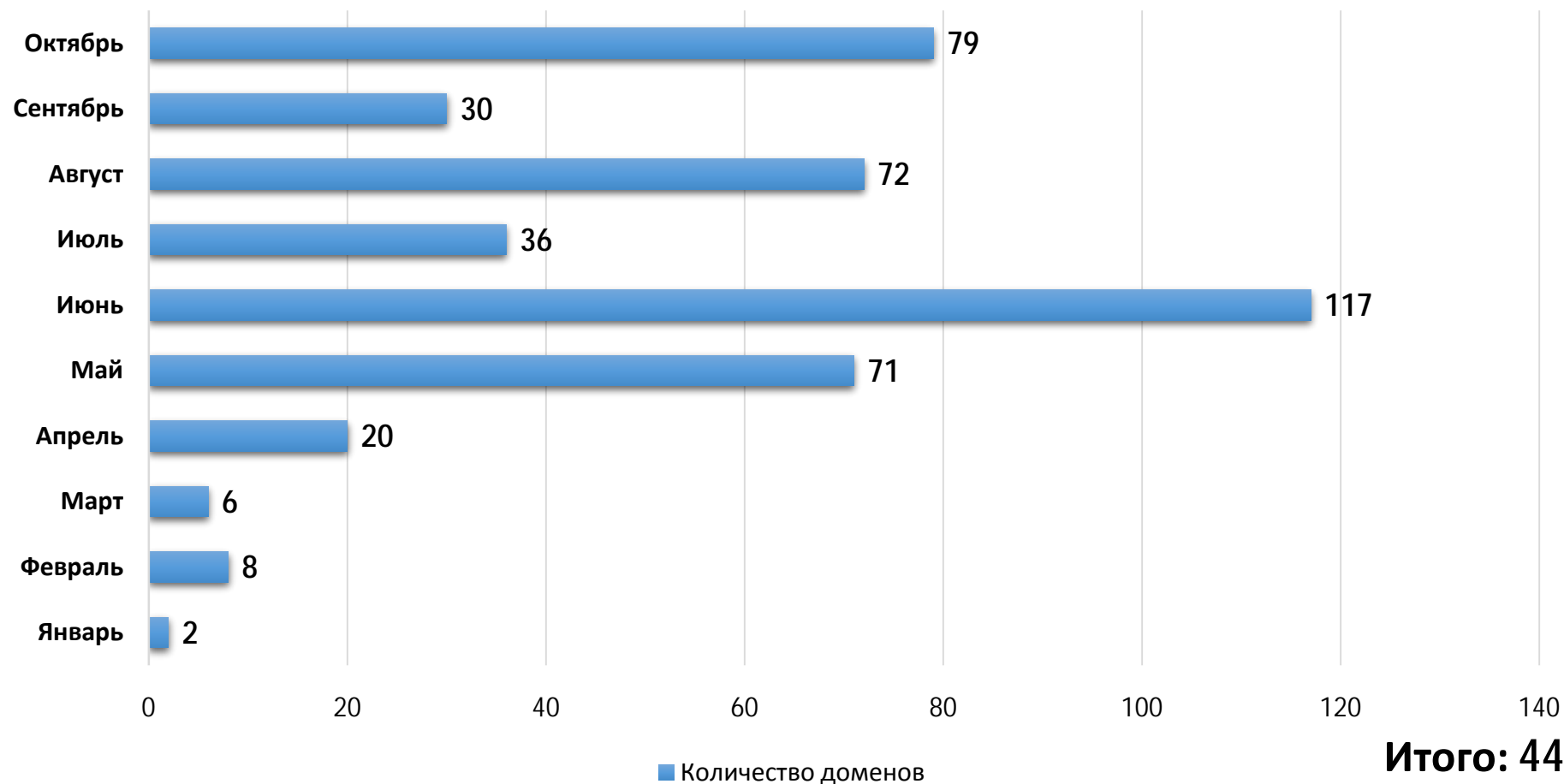
предотвратили хищений на **~0,57** млрд. руб.



Перспективные направления

Антифишинг & Антиспам

Количество доменов направленных на блокировку с начала 2016 г.



Перспективные направления

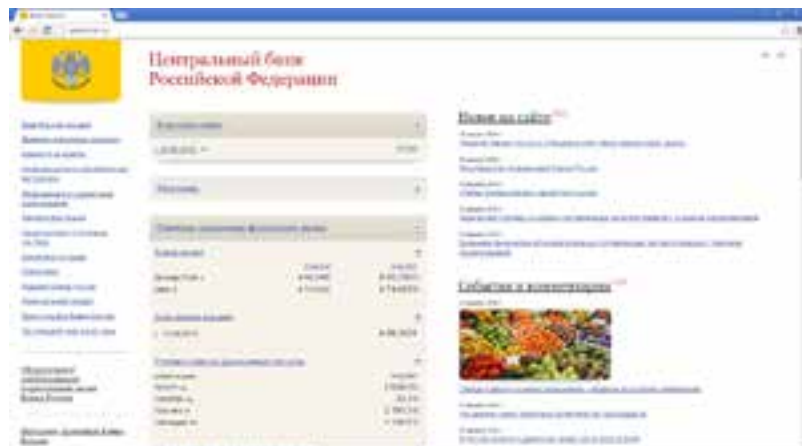
Антифрод



Усиление технической экспертизы



Внедрение системы личных кабинетов



Гражданские правоотношения



Международное сотрудничество





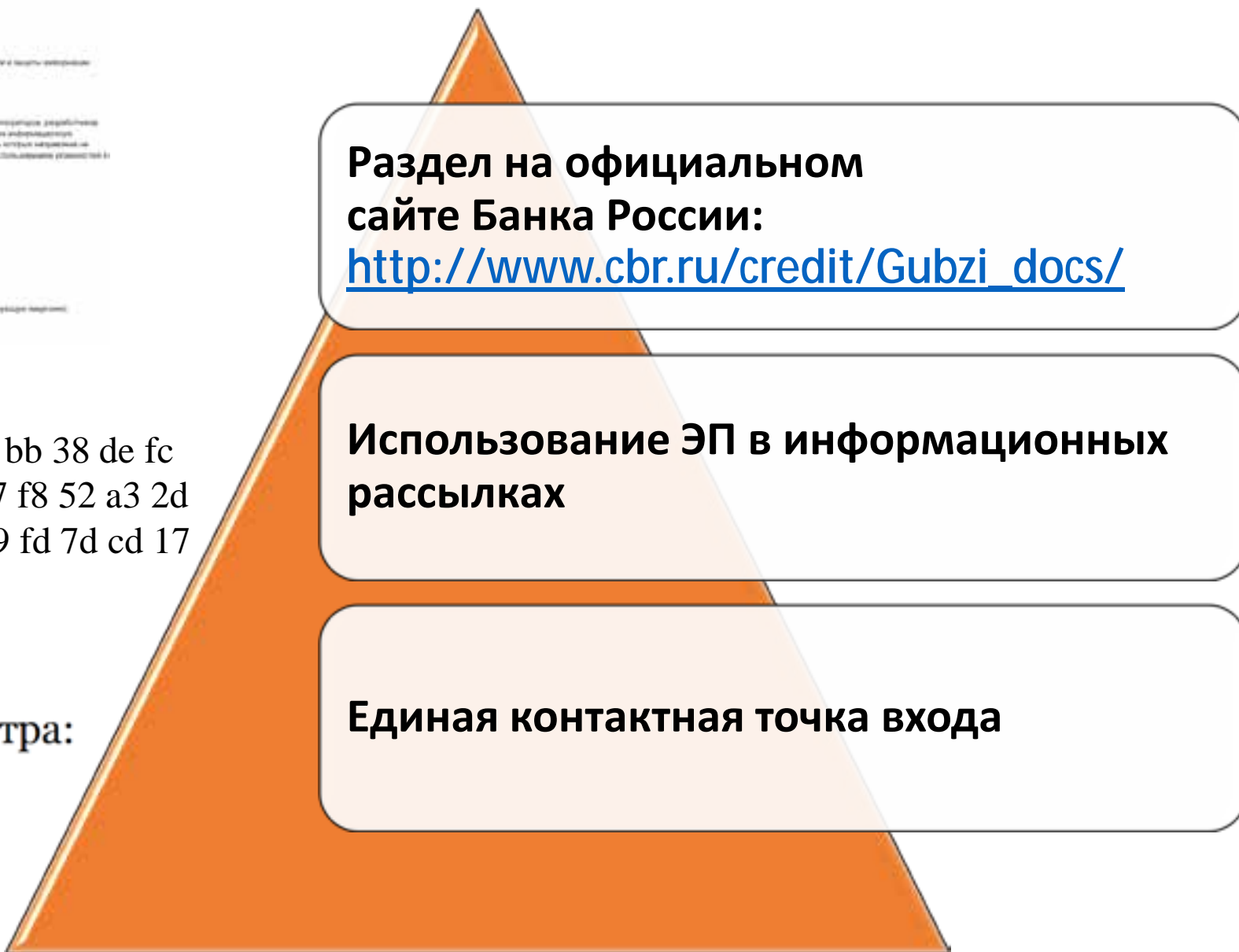
Отпечаток открытого ключа ЭП

04 40 9e af 6f 1b d1 f3 cb b9 9b 03 fc c2 76 0b bb 38 de fc
65 e9 d0 b7 bd 76 5e c4 bf df 47 58 3d a4 1c 77 f8 52 a3 2d
7c 1e 65 b3 1f 52 bc 5a 75 d8 93 cb 00 d1 ac 89 fd 7d cd 17
db e2 01 cb f6 21

По любым возникающим вопросам
можно связаться с работниками Центра:

Телефон: +7 (495) 772-70-90

E-mail: info_fincert@cbr.ru





Банк России

Центральный банк Российской Федерации



Спасибо за внимание!

Д.Б. Фролов - начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России

E-mail : fdb@cbr.ru

Тел.: +7 (495) 772-70-96