БАНК РОССИИ
ФИНЦЕРТ

19 сентября 2017 года

FinCERT: Цели и задачи.

А.И. КАЛАШНИКОВ
FinCERT Банка России

Основные задачи FinCERT

Установление и совершенствование методологии противодействия противоправным действиям при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий и противодействия компьютерным атакам на информационные ресурсы организаций, поднадзорных Банку России, в части:

- **установления требований и рекомендаций в области обеспечения защиты информации в организациях, поднадзорных Банку России;**
- **установления состава и содержания сведений, используемых в рамках информационного обмена между Банком России, организациями, поднадзорными Банку России, и правоохранительными органами;**
- **установления порядка осуществления контроля в рамках надзора за соблюдением требований Банка России в области обеспечения защиты информации в организациях поднадзорных Банку России.**

Основные задачи FinCERT (продолжение)

Проведение информационно-аналитической работы, направленной на совершенствование методов противодействия компьютерным атакам при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий, в том числе в рамках противодействия компьютерным атакам на информационные ресурсы организаций, поднадзорных Банку России в части:

- **анализа данных о фактах проявления противоправных действий при осуществлении переводов денежных средств в национальной платежной системе, включая компьютерные атаки на организации, поднадзорные Банку России, рисках, связанных с обеспечением безопасности;**
- **своевременного формирования оперативных рекомендаций по снижению рисков, связанных с обеспечением безопасности при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий.**
- **повышение киберграмотности и участие в разработке учебных программ для ВУЗов, школ.**

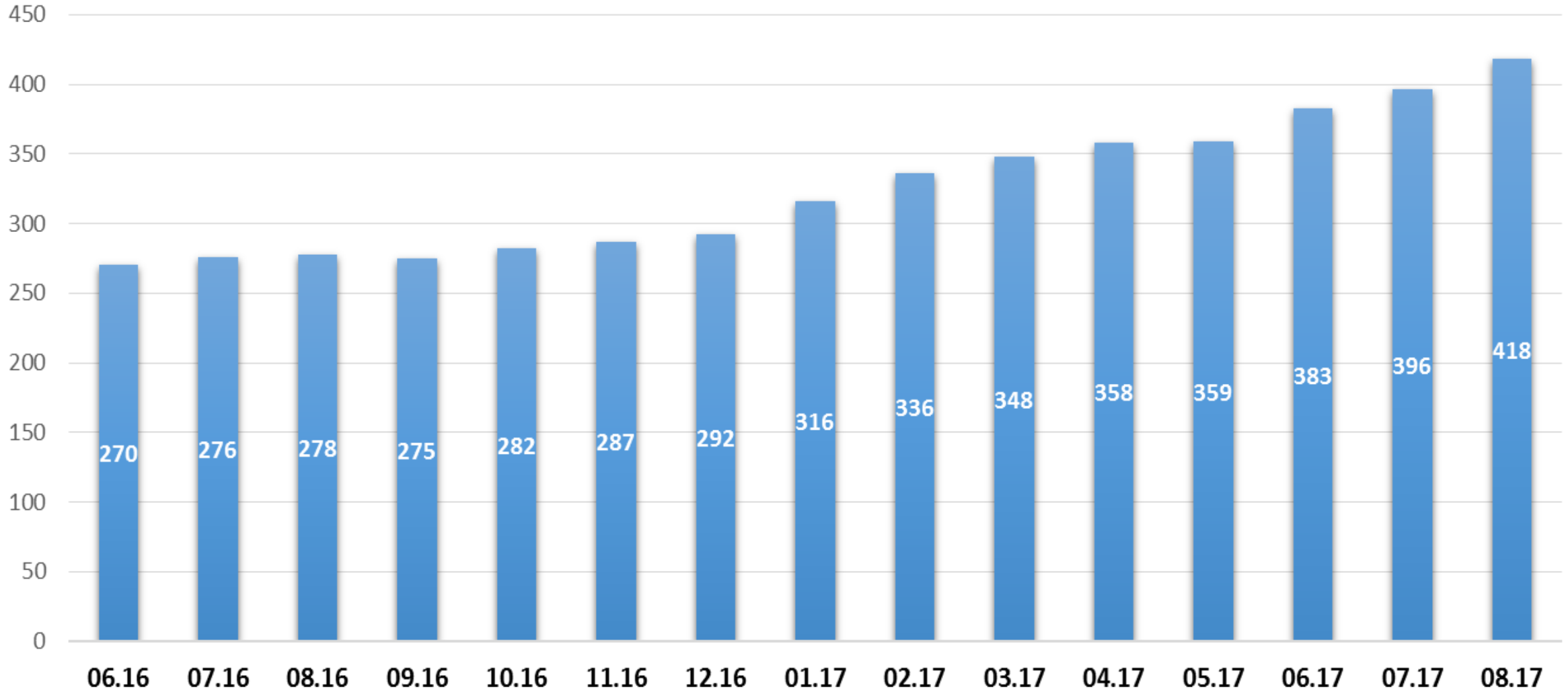
Основные принципы деятельности FinCERT

Добровольность

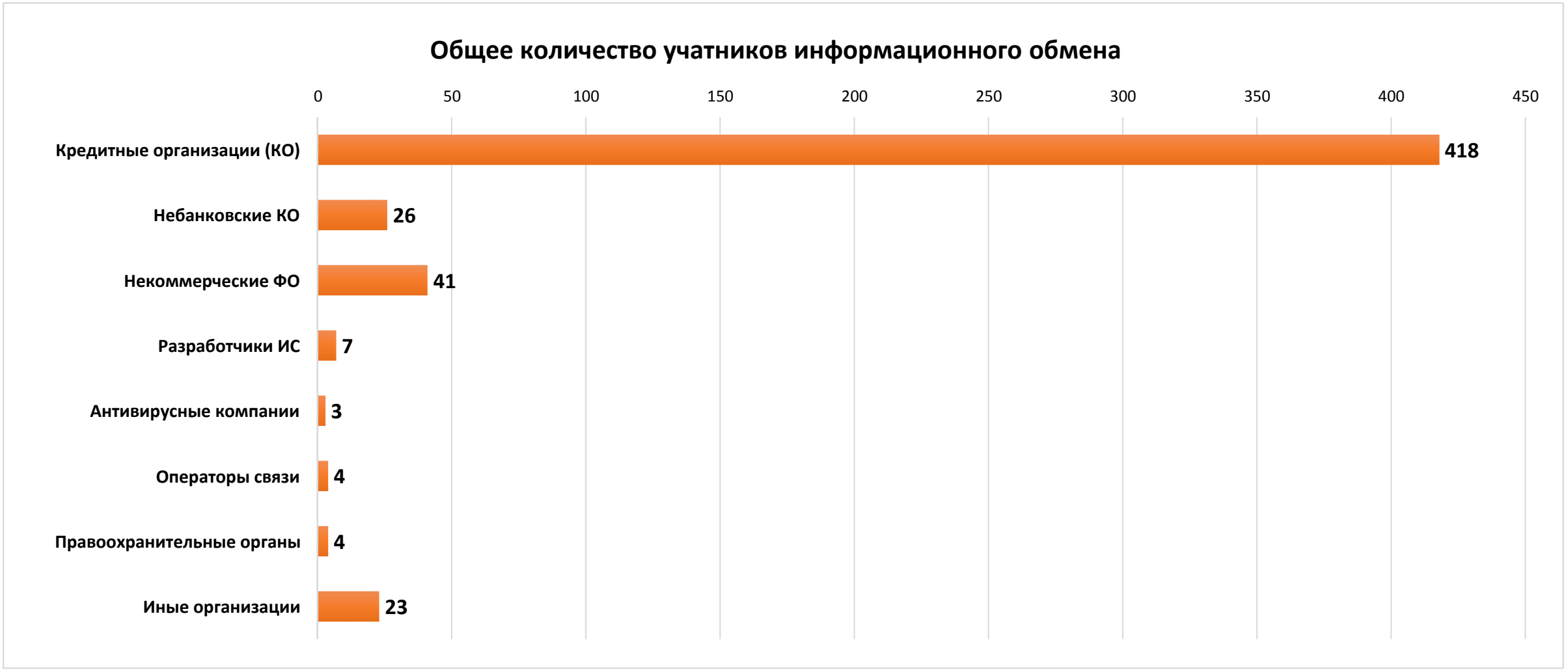
Открытость

Доверие

Динамика присоединения кредитных организаций к информационному обмену



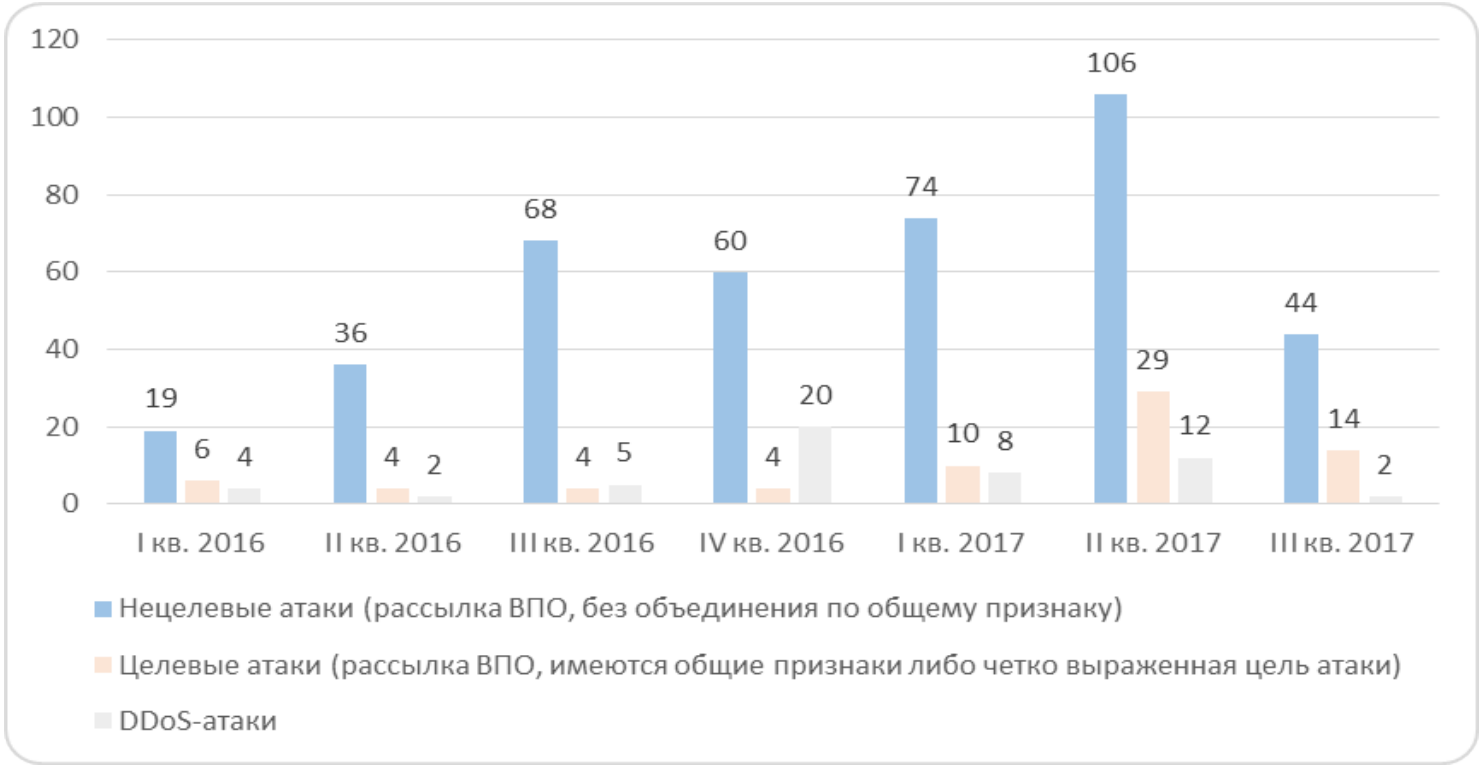
Состав участников информационного обмена



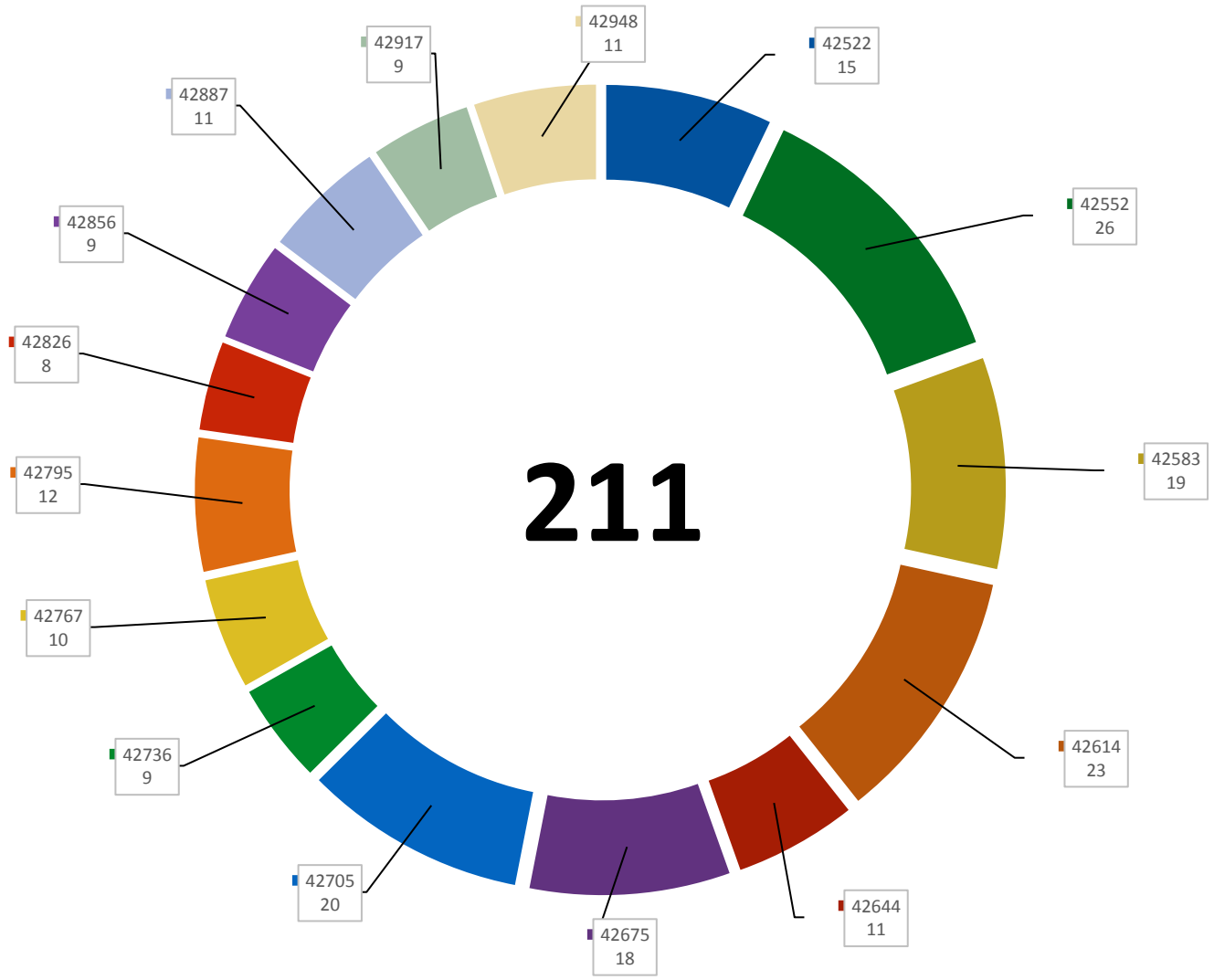
Всего 526 участников

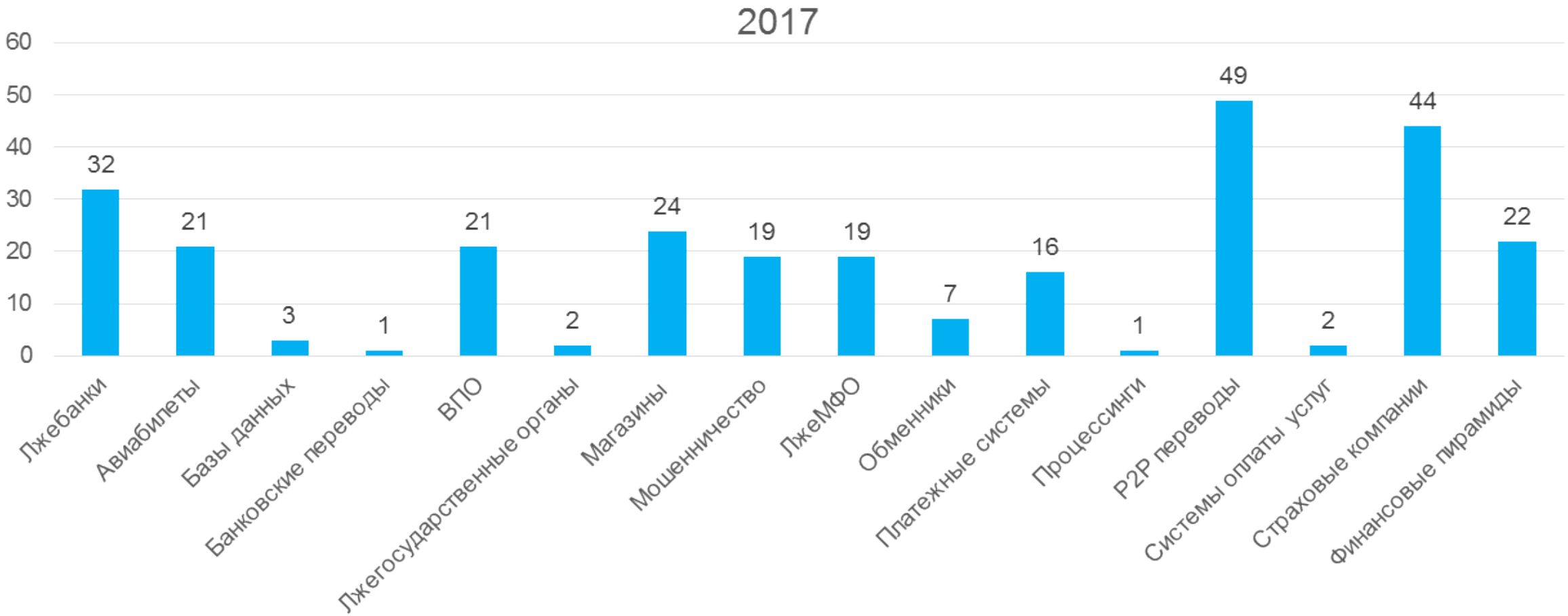
Число кампаний (типов атак), направленных на организации кредитно-финансовой сферы, по статистике FinCERT

- **407** нецелевых атак (массовая рассылка ВПО или ссылок на загрузку ВПО; признаки, позволяющие классифицировать атаку как целевую, отсутствовали;
- **71** целевую атаку (были обнаружены признаки, позволяющие объединить несколько фишинговых кампаний в рамках одной выделенной целевой атаки или предположить, что атака организована одной группой);
- **53** случаев атак типа «Отказ в обслуживании» (DDoS).



Итоговые данные за 2016 - 2017 г. по числу выполненных рассылок информационных бюллетеней





ФинЦЕРТ как уполномоченная организация уведомляет регистраторов доменных имен о доменах, с которых рассылается вредоносный код и осуществляются мошеннические действия, связанные с использованием платежных карт.

Информационная рассылка ФинЦЕРТ

БАНК РОССИИ ФИНЦЕРТ ФинЦЕРТ Банка России ИР-20170804

M-VA:OTH-BANKER_SVPENG-20170804-01:i

Банковский троян Trojan-Banker.AndroidOS.Svpeng.ae

Описание угрозы	Обнаружена обновленная версия банковского троянского ПО Trojan-Banker.AndroidOS.Svpeng.ae, распространяемая через вредоносные сайты, в качестве поддельного Flash-проигрывателя (ранее выявлявшиеся версии распространялись через AdSense, используя уязвимость в браузере Chrome).
На что направлена	Мобильные устройства на Android
Способ реализации	После запуска вредоносное ПО Trojan-Banker.AndroidOS.Svpeng.ae проверяет язык интерфейса устройства и, если используемый язык не является русским, запрашивает разрешение на использование специальных возможностей. Используя данную привилегию, Trojan-Banker.AndroidOS.Svpeng.ae выполняет множество вредоносных действий: ПО предоставляет себе права администратора устройства, выдает права на показ окон ПО поверх остальных приложений, устанавливает себя в качестве SMS-приложения по умолчанию и предоставляет несколько динамических разрешений, которые позволяют получать и отправлять SMS-сообщения, совершать вызовы и просматривать список контактов. Более того, используя полученные возможности, Trojan-Banker.AndroidOS.Svpeng.ae может блокировать любую попытку лишить его прав администратора устройства, предотвращая деинсталляцию. Тем самым он блокирует любую попытку добавить или удалить права администратора устройства, в том числе для любого другого приложения. С помощью специальных возможностей вредоносное ПО получает доступ к

Email: fincert@cbr.ru

- описание угрозы
- вектор атаки
- способы реализации
- базовые меры по противодействию

FinCERT Банка России

PC-V-BD-VAR_BACKDOOR-20170809-01

Рассылка информации о рассылке ВПО

1. Краткое описание угрозы

Зафиксирована рассылка вредоносного программного обеспечения, имеющего признаки backdoor.

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	На 09.08.2017 не определяется абсолютным большинством антивирусных решений
2	Блокировка запросов	h**p://137.74.224.142
3	Блокировка отправителей	nikolaj.voronczov.61@mail.ru

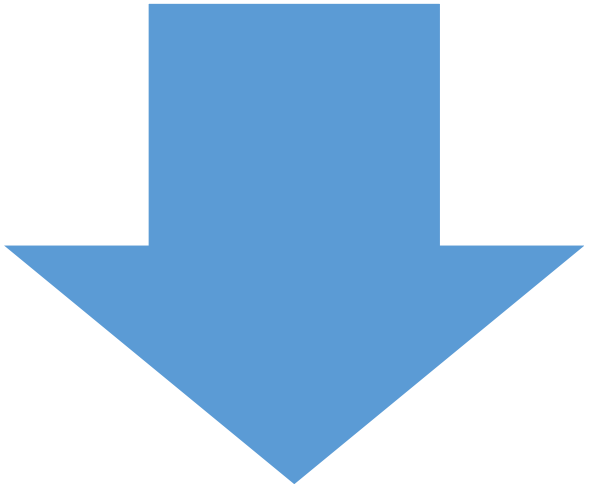
3. Индикаторы компрометации

Индикаторы компрометации *(загружаемые файлы, SHA1)*:

Хэш- сумма	Имя файла	Размер, байт
SHA: A52DED0AC2F4207DCD23036EFD9D845ADD972541 **MD5:** 667C7F50177A64B4CB30AAD8D4D0360E	выписка по счету клиента.docx	1008026
SHA: 6C3D8013B6FADEB7BC9F9C356636E06287024301 **MD5:** 3345DDE0C827DCBDA993F7216A8D7C12	IntelSofts_*.exe	64000

Email: fincert@cbr.ru

- описание угрозы
- базовые меры по противодействию
- индикаторы компрометации
- сведения об источниках (отправителе)

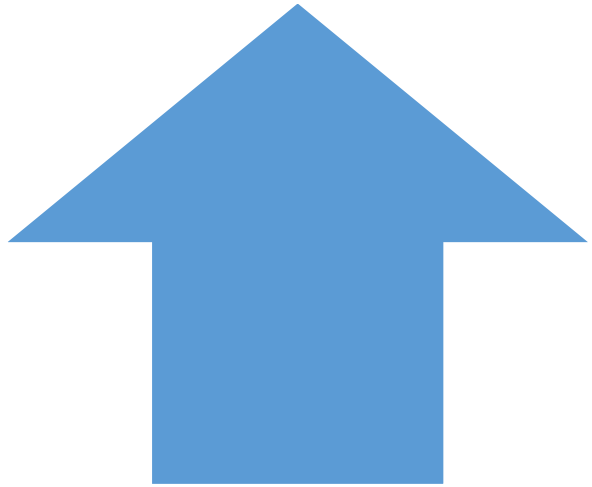


Снято с делегирования доменов

- **2016 г.: 100**
- **2017 г. 376 (**отправлено 481**)**

Отправлено для добавления в «черные списки» (ГосСОПКА, антивирусные лаборатории, поисковые системы)

- **2016 г.: 1601**
- **2017 г. 120 759**

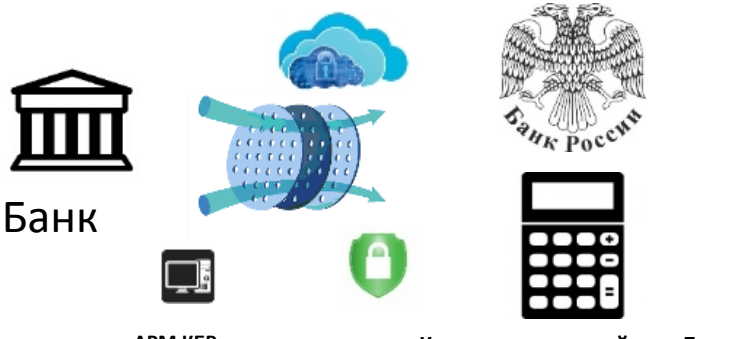


Основная проблематика

- **Отсутствие единого компетентного центра блокировки мошеннических ресурсов**
- **Отсутствие заинтересованности со стороны поставщиков услуг и отсутствие требований к ним со стороны регулятора**
- **Сложности при проведении расследования правоохранительными органами**

Перспективные направления

Антифрод



Усиление технической

Проверки поднадзорных организаций

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

9 июня 2012 г. № 382-П

г. Москва

П О Л О Ж Е Н И Е

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Глава 1. **Общие положения**

1.1. На основании Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) (далее – Федеральный закон № 161-ФЗ) настоящее Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее – требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

Внедрение системы личных кабинетов

Гражданские правоотношения

Международное сотрудничество

FIRST
Improving Security Together

ЕАЭС Евразийский экономический союз

E.A.S.T

enisa
European Network and Information Security Agency

БАНК РОССИИ
ФИНЦЕРТ

Спасибо за внимание!

А.И. КАЛАШНИКОВ - начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России

E-mail : kai2@cbr.ru

Тел.: +7 (495) 957-83-04