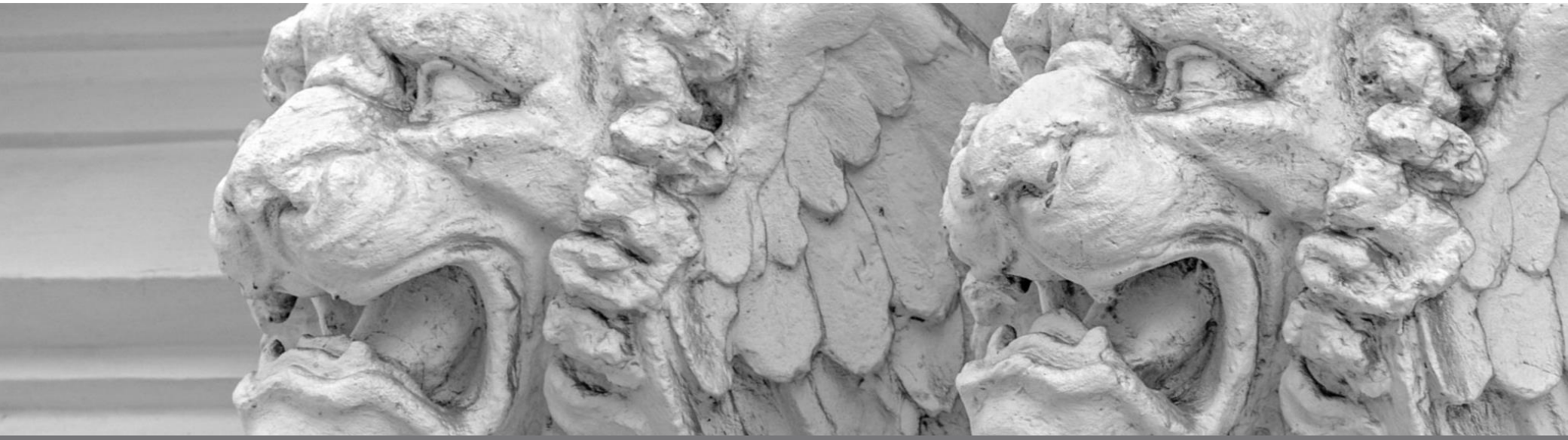
Банк России
Центральный банк Российской Федерации



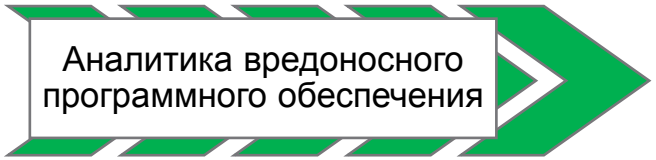
Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России. Взгляд изнутри

Сударенко Артем
ГУБиЗИ Банка России

Общая схема работы

Получение исходных данных

Работа аналитиков



экземпляр вредоносного ПО

- Определение детектируемости антивирусными программными средствами по данным VirusTotal
- Определение маркеров заражения

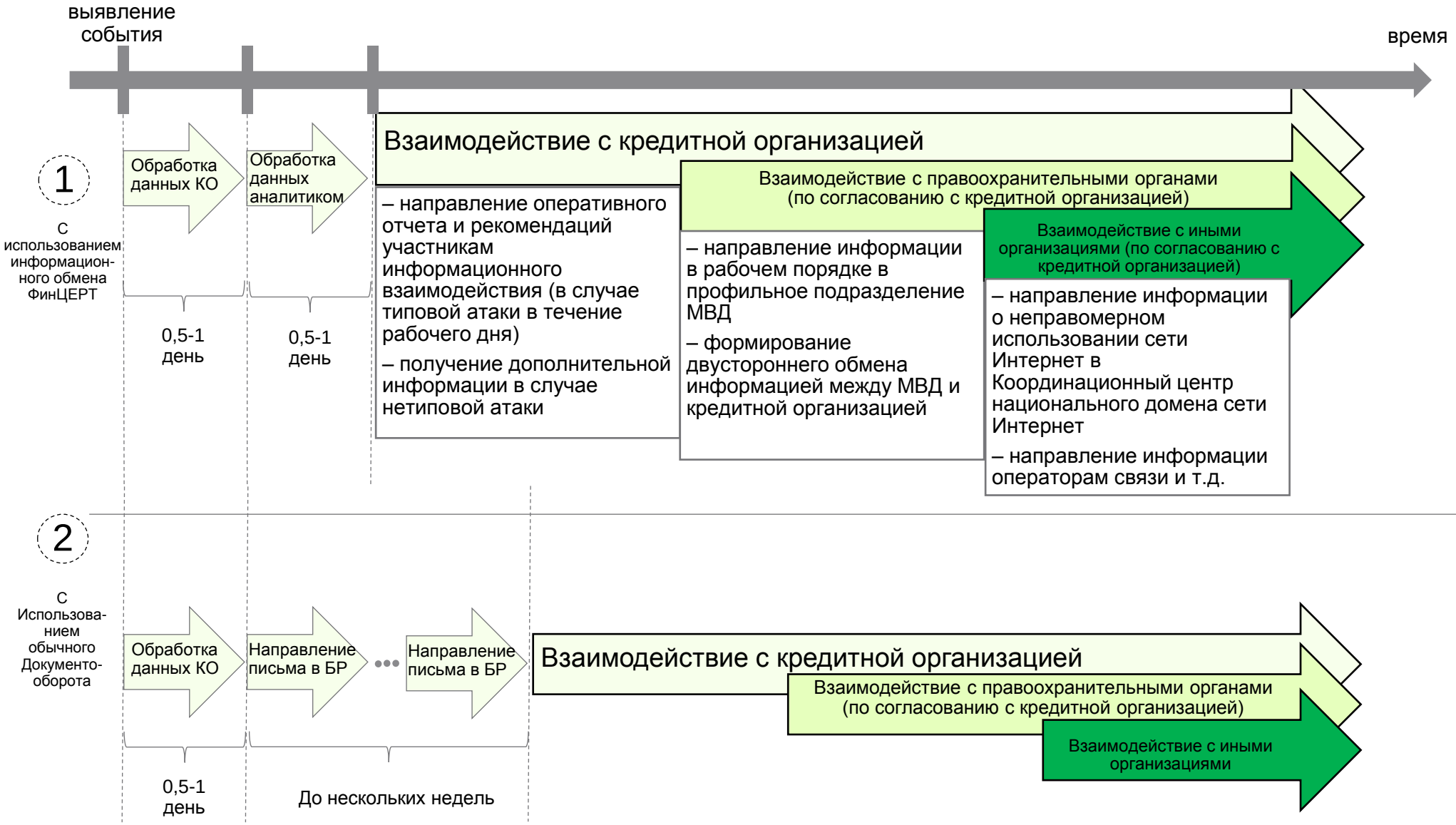
лог-файлы и образы дисков

- Выявление нестандартной сетевой активности
- Выявление нестандартных действий локальных пользователей

бизнес-процессы

- Сопоставление существующих бизнес-процессов и полученных в результате технической аналитики данных

Рассмотрение обращения, подготовка оперативных отчетов и рекомендаций



Обратная связь

Банк России
Центральный банк Российской Федерации

Спасибо за внимание!

Сударенко Артем Александрович **(Консультант Центра)**	**E-mail**	**SudarenkoAA@cbr.ru** **FinCERT@cbr.ru**
	Тел.	+7 (495) 771-99-99 доб. 1-55-98