



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







Аналитика вредоносного программного обеспечения

экземпляр вредоносного ПО

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

Техническая аналитика

лог-файлы и образы дисков

- Выявление нестандартной сетевой активности
- Выявление нестандартных действий локальных пользователей

Аналитика бизнес-процессов

бизнес-процессы

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



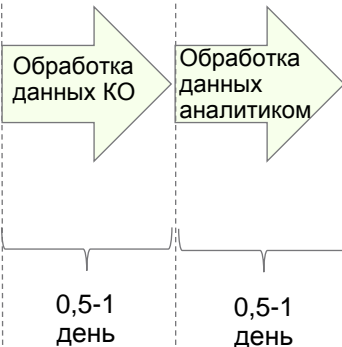
Рассмотрение обращения, подготовка оперативных отчетов и рекомендаций

выявление
события

время

1

С использованием информационного обмена ФИНЦЕРТ



Взаимодействие с кредитной организацией

- направление оперативного отчета и рекомендаций участникам информационного взаимодействия (в случае типовой атаки в течение рабочего дня)
- получение дополнительной информации в случае нетиповой атаки

Взаимодействие с правоохранительными органами (по согласованию с кредитной организацией)

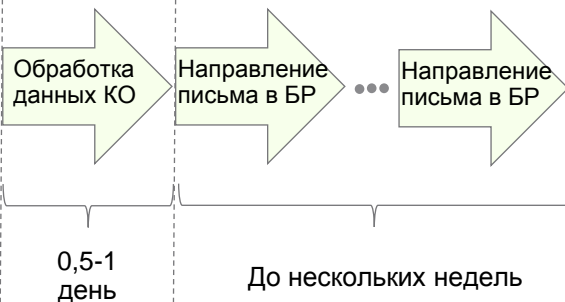
- направление информации в рабочем порядке в профильное подразделение МВД
- формирование двустороннего обмена информацией между МВД и кредитной организацией

Взаимодействие с иными организациями (по согласованию с кредитной организацией)

- направление информации о неправомерном использовании сети Интернет в Координационный центр национального домена сети Интернет
- направление информации операторам связи и т.д.

2

С использованием обычного Документо-оборота



Взаимодействие с кредитной организацией

Взаимодействие с правоохранительными органами (по согласованию с кредитной организацией)

Взаимодействие с иными организациями



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