



# АСОИ ФинЦЕРТ – платформа Банка России по обработке инцидентов

БАНК РОССИИ



1. Изменения нормативной базы
  - Федеральный закон от 26.07.2017 N 187-ФЗ и Федеральный закон от 27.06.2018 N 167-ФЗ;
  - Положения Банка России №382-П и Положения Банка России №552-П.
2. Актуальные вопросы при взаимодействии с участниками обмена
  - отсутствие единого способа взаимодействия с участниками (события, форматы, меры реагирования и т.д.);
  - взаимодействие с участниками с использованием e-mail;
  - отсутствие автоматизации обработки сведений об инцидентах, поступающих от Участников;
  - отсутствие ресурса, содержащего актуальную информацию об атаках, осуществляемых на организации кредитно-финансовой сферы (в том числе содержащих индикаторы компрометации рекомендации по выявлению и предотвращению и т.д.);
3. Активизация киберпреступников и необходимость активных мер по реагированию на актуальные угрозы ИБ
  - распространение целевых атак;
  - широкомасштабное появление мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере и сайтов, распространяющих вредоносное программное обеспечение.

- Создание информационно-сервисного портала и личных кабинетов для взаимодействия с Участниками обмена;
- Обеспечение инфраструктуры защищенного доверенного взаимодействия;
- Автоматизация обработки сведений об инцидентах, поступающих от Участников;
- Обеспечение возможности передачи информации об инцидентах (для выполнения 167-ФЗ и 187-ФЗ (передача информации в ГосСОПКА через ФинЦЕРТ));
- ведение базы знаний по уязвимостям, индикаторам компрометации, индикаторам компрометации ("паттернам") атак, ведение архива расследований инцидентов ИБ и запросов участников;
- мониторинг электронных СМИ с целью выявления информации, связанной с подготовкой и реализацией атак на организации кредитно-финансовой сферы

## Получение информации (данных) от Участника

Получение данных от Участника через ЛК (интерактивный ввод данных)

Получение данных от Участника через ЛК (интерактивный ввод пакетов данных об инцидентах)

Получение данных от Участника через e-mail (в фиксированном формате)

Получение данных от Участника в автоматическом режиме (2-я очередь)

## Передача информации (данных) Участнику

информирование Участников об актуальных угрозах ИБ в КФС (распространение бюллетеней)

Взаимодействие с участником по запросам и инцидентам, переданным в ФинЦЕРТ

Передача данных об угрозах/инцидентах

## Проведение мониторинга информационных ресурсов Интернет

поиск мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере

мониторинг информационных атак на организации КФС

## Обработка информации о компьютерных атаках

поддержка процедур реагирования и расследования

поддержка взаимодействия с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов

<#>

[illegible]



# Функционирование АСОИ ФинЦЕРТ: Что получает участник обмена

## Информационные бюллетени

## Предупреждения об уязвимостях

ИР-20180609

ФИНЦЕРТ

1

РС- ОН:ВН-  
BACKSWAP-  
20180609-013

Троянская программа BackSwap использует новые способы кражи средств с банковских счетов.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Описание угрозы             | Специалисты ESET обнаружили новое семейство троянских программ, использующее относительно новый способ кражи средств с банковских счетов. BackSwap «работает» с элементами графического интерфейса Windows и имитирует нажатия клавиш, чтобы избежать обнаружения и обойти защиту браузера.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| На что направлена           | ПК пользователя                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Способ реализации           | BackSwap распространяется посредством фишинговых рассылок. В письмах содержатся вложения с маскированным (обфусцированным) JavaScript-загрузчиком из семейства Neticod.<br>Полезная нагрузка BackSwap доставляется в систему в виде модифицированной версии легитимного приложения, частично переписанного вредоносным компонентом. Обнаружив работу с интернет-банком, BackSwap внедряет вредоносный код в веб-страницу через консоль разработчика в браузере или в адресную строку.<br>Таким образом вредоносный скрипт выполняется напрямую из адресной строки с применением малоиспользуемой функции JavaScript. Вредоносное ПО имитирует нажатие CTRL+L для выбора адресной строки, DELETE – для очистки поля, «вводит» символы на «javascript» через вызов SendMessageA в цикле, после чего вставляет вредоносный скрипт с помощью комбинации CTRL+V. Скрипт выполняется после «нажатия» ENTER. В конце процесса адресная строка очищается, чтобы убрать следы компрометации. |
| Дата выявления / публикации | 05.06.2018                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Email: [fincert@cdr.ru](mailto:fincert@cdr.ru)

1

ФИНЦЕРТ

ИР-20180609-001

### Предупреждение об уязвимости некоторых устройств Cisco

#### 1. Краткое описание угрозы

Зафиксированы случаи использования RC2 (Remote Code Execution – удаленное исполнение кода) уязвимости в Cisco IOS и Cisco IOS XE.

Атакующие настраивают bot-сети на сканирование устройств с открытыми портами TCP/4786 (уязвимость в Cisco IOS Smart Install, CVE-2018-0171, CVE-2018-0172, CVE-2018-0173, CVE-2018-0174, CVE-2018-0175, CVE-2018-0176, CVE-2018-0177, CVE-2018-0178, CVE-2018-0179, CVE-2018-0180, CVE-2018-0181, CVE-2018-0182, CVE-2018-0183, CVE-2018-0184, CVE-2018-0185, CVE-2018-0186, CVE-2018-0187, CVE-2018-0188, CVE-2018-0189, CVE-2018-0190, CVE-2018-0191, CVE-2018-0192, CVE-2018-0193, CVE-2018-0194, CVE-2018-0195, CVE-2018-0196, CVE-2018-0197, CVE-2018-0198, CVE-2018-0199, CVE-2018-0200, CVE-2018-0201, CVE-2018-0202, CVE-2018-0203, CVE-2018-0204, CVE-2018-0205, CVE-2018-0206, CVE-2018-0207, CVE-2018-0208, CVE-2018-0209, CVE-2018-0210, CVE-2018-0211, CVE-2018-0212, CVE-2018-0213, CVE-2018-0214, CVE-2018-0215, CVE-2018-0216, CVE-2018-0217, CVE-2018-0218, CVE-2018-0219, CVE-2018-0220, CVE-2018-0221, CVE-2018-0222, CVE-2018-0223, CVE-2018-0224, CVE-2018-0225, CVE-2018-0226, CVE-2018-0227, CVE-2018-0228, CVE-2018-0229, CVE-2018-0230, CVE-2018-0231, CVE-2018-0232, CVE-2018-0233, CVE-2018-0234, CVE-2018-0235, CVE-2018-0236, CVE-2018-0237, CVE-2018-0238, CVE-2018-0239, CVE-2018-0240, CVE-2018-0241, CVE-2018-0242, CVE-2018-0243, CVE-2018-0244, CVE-2018-0245, CVE-2018-0246, CVE-2018-0247, CVE-2018-0248, CVE-2018-0249, CVE-2018-0250, CVE-2018-0251, CVE-2018-0252, CVE-2018-0253, CVE-2018-0254, CVE-2018-0255, CVE-2018-0256, CVE-2018-0257, CVE-2018-0258, CVE-2018-0259, CVE-2018-0260, CVE-2018-0261, CVE-2018-0262, CVE-2018-0263, CVE-2018-0264, CVE-2018-0265, CVE-2018-0266, CVE-2018-0267, CVE-2018-0268, CVE-2018-0269, CVE-2018-0270, CVE-2018-0271, CVE-2018-0272, CVE-2018-0273, CVE-2018-0274, CVE-2018-0275, CVE-2018-0276, CVE-2018-0277, CVE-2018-0278, CVE-2018-0279, CVE-2018-0280, CVE-2018-0281, CVE-2018-0282, CVE-2018-0283, CVE-2018-0284, CVE-2018-0285, CVE-2018-0286, CVE-2018-0287, CVE-2018-0288, CVE-2018-0289, CVE-2018-0290, CVE-2018-0291, CVE-2018-0292, CVE-2018-0293, CVE-2018-0294, CVE-2018-0295, CVE-2018-0296, CVE-2018-0297, CVE-2018-0298, CVE-2018-0299, CVE-2018-0300, CVE-2018-0301, CVE-2018-0302, CVE-2018-0303, CVE-2018-0304, CVE-2018-0305, CVE-2018-0306, CVE-2018-0307, CVE-2018-0308, CVE-2018-0309, CVE-2018-0310, CVE-2018-0311, CVE-2018-0312, CVE-2018-0313, CVE-2018-0314, CVE-2018-0315, CVE-2018-0316, CVE-2018-0317, CVE-2018-0318, CVE-2018-0319, CVE-2018-0320, CVE-2018-0321, CVE-2018-0322, CVE-2018-0323, CVE-2018-0324, CVE-2018-0325, CVE-2018-0326, CVE-2018-0327, CVE-2018-0328, CVE-2018-0329, CVE-2018-0330, CVE-2018-0331, CVE-2018-0332, CVE-2018-0333, CVE-2018-0334, CVE-2018-0335, CVE-2018-0336, CVE-2018-0337, CVE-2018-0338, CVE-2018-0339, CVE-2018-0340, CVE-2018-0341, CVE-2018-0342, CVE-2018-0343, CVE-2018-0344, CVE-2018-0345, CVE-2018-0346, CVE-2018-0347, CVE-2018-0348, CVE-2018-0349, CVE-2018-0350, CVE-2018-0351, CVE-2018-0352, CVE-2018-0353, CVE-2018-0354, CVE-2018-0355, CVE-2018-0356, CVE-2018-0357, CVE-2018-0358, CVE-2018-0359, CVE-2018-0360, CVE-2018-0361, CVE-2018-0362, CVE-2018-0363, CVE-2018-0364, CVE-2018-0365, CVE-2018-0366, CVE-2018-0367, CVE-2018-0368, CVE-2018-0369, CVE-2018-0370, CVE-2018-0371, CVE-2018-0372, CVE-2018-0373, CVE-2018-0374, CVE-2018-0375, CVE-2018-0376, CVE-2018-0377, CVE-2018-0378, CVE-2018-0379, CVE-2018-0380, CVE-2018-0381, CVE-2018-0382, CVE-2018-0383, CVE-2018-0384, CVE-2018-0385, CVE-2018-0386, CVE-2018-0387, CVE-2018-0388, CVE-2018-0389, CVE-2018-0390, CVE-2018-0391, CVE-2018-0392, CVE-2018-0393, CVE-2018-0394, CVE-2018-0395, CVE-2018-0396, CVE-2018-0397, CVE-2018-0398, CVE-2018-0399, CVE-2018-0400, CVE-2018-0401, CVE-2018-0402, CVE-2018-0403, CVE-2018-0404, CVE-2018-0405, CVE-2018-0406, CVE-2018-0407, CVE-2018-0408, CVE-2018-0409, CVE-2018-0410, CVE-2018-0411, CVE-2018-0412, CVE-2018-0413, CVE-2018-0414, CVE-2018-0415, CVE-2018-0416, CVE-2018-0417, CVE-2018-0418, CVE-2018-0419, CVE-2018-0420, CVE-2018-0421, CVE-2018-0422, CVE-2018-0423, CVE-2018-0424, CVE-2018-0425, CVE-2018-0426, CVE-2018-0427, CVE-2018-0428, CVE-2018-0429, CVE-2018-0430, CVE-2018-0431, CVE-2018-0432, CVE-2018-0433, CVE-2018-0434, CVE-2018-0435, CVE-2018-0436, CVE-2018-0437, CVE-2018-0438, CVE-2018-0439, CVE-2018-0440, CVE-2018-0441, CVE-2018-0442, CVE-2018-0443, CVE-2018-0444, CVE-2018-0445, CVE-2018-0446, CVE-2018-0447, CVE-2018-0448, CVE-2018-0449, CVE-2018-0450, CVE-2018-0451, CVE-2018-0452, CVE-2018-0453, CVE-2018-0454, CVE-2018-0455, CVE-2018-0456, CVE-2018-0457, CVE-2018-0458, CVE-2018-0459, CVE-2018-0460, CVE-2018-0461, CVE-2018-0462, CVE-2018-0463, CVE-2018-0464, CVE-2018-0465, CVE-2018-0466, CVE-2018-0467, CVE-2018-0468, CVE-2018-0469, CVE-2018-0470, CVE-2018-0471, CVE-2018-0472, CVE-2018-0473, CVE-2018-0474, CVE-2018-0475, CVE-2018-0476, CVE-2018-0477, CVE-2018-0478, CVE-2018-0479, CVE-2018-0480, CVE-2018-0481, CVE-2018-0482, CVE-2018-0483, CVE-2018-0484, CVE-2018-0485, CVE-2018-0486, CVE-2018-0487, CVE-2018-0488, CVE-2018-0489, CVE-2018-0490, CVE-2018-0491, CVE-2018-0492, CVE-2018-0493, CVE-2018-0494, CVE-2018-0495, CVE-2018-0496, CVE-2018-0497, CVE-2018-0498, CVE-2018-0499, CVE-2018-0500, CVE-2018-0501, CVE-2018-0502, CVE-2018-0503, CVE-2018-0504, CVE-2018-0505, CVE-2018-0506, CVE-2018-0507, CVE-2018-0508, CVE-2018-0509, CVE-2018-0510, CVE-2018-0511, CVE-2018-0512, CVE-2018-0513, CVE-2018-0514, CVE-2018-0515, CVE-2018-0516, CVE-2018-0517, CVE-2018-0518, CVE-2018-0519, CVE-2018-0520, CVE-2018-0521, CVE-2018-0522, CVE-2018-0523, CVE-2018-0524, CVE-2018-0525, CVE-2018-0526, CVE-2018-0527, CVE-2018-0528, CVE-2018-0529, CVE-2018-0530, CVE-2018-0531, CVE-2018-0532, CVE-2018-0533, CVE-2018-0534, CVE-2018-0535, CVE-2018-0536, CVE-2018-0537, CVE-2018-0538, CVE-2018-0539, CVE-2018-0540, CVE-2018-0541, CVE-2018-0542, CVE-2018-0543, CVE-2018-0544, CVE-2018-0545, CVE-2018-0546, CVE-2018-0547, CVE-2018-0548, CVE-2018-0549, CVE-2018-0550, CVE-2018-0551, CVE-2018-0552, CVE-2018-0553, CVE-2018-0554, CVE-2018-0555, CVE-2018-0556, CVE-2018-0557, CVE-2018-0558, CVE-2018-0559, CVE-2018-0560, CVE-2018-0561, CVE-2018-0562, CVE-2018-0563, CVE-2018-0564, CVE-2018-0565, CVE-2018-0566, CVE-2018-0567, CVE-2018-0568, CVE-2018-0569, CVE-2018-0570, CVE-2018-0571, CVE-2018-0572, CVE-2018-0573, CVE-2018-0574, CVE-2018-0575, CVE-2018-0576, CVE-2018-0577, CVE-2018-0578, CVE-2018-0579, CVE-2018-0580, CVE-2018-0581, CVE-2018-0582, CVE-2018-0583, CVE-2018-0584, CVE-2018-0585, CVE-2018-0586, CVE-2018-0587, CVE-2018-0588, CVE-2018-0589, CVE-2018-0590, CVE-2018-0591, CVE-2018-0592, CVE-2018-0593, CVE-2018-0594, CVE-2018-0595, CVE-2018-0596, CVE-2018-0597, CVE-2018-0598, CVE-2018-0599, CVE-2018-0600, CVE-2018-0601, CVE-2018-0602, CVE-2018-0603, CVE-2018-0604, CVE-2018-0605, CVE-2018-0606, CVE-2018-0607, CVE-2018-0608, CVE-2018-0609, CVE-2018-0610, CVE-2018-0611, CVE-2018-0612, CVE-2018-0613, CVE-2018-0614, CVE-2018-0615, CVE-2018-0616, CVE-2018-0617, CVE-2018-0618, CVE-2018-0619, CVE-2018-0620, CVE-2018-0621, CVE-2018-0622, CVE-2018-0623, CVE-2018-0624, CVE-2018-0625, CVE-2018-0626, CVE-2018-0627, CVE-2018-0628, CVE-2018-0629, CVE-2018-0630, CVE-2018-0631, CVE-2018-0632, CVE-2018-0633, CVE-2018-0634, CVE-2018-0635, CVE-2018-0636, CVE-2018-0637, CVE-2018-0638, CVE-2018-0639, CVE-2018-0640, CVE-2018-0641, CVE-2018-0642, CVE-2018-0643, CVE-2018-0644, CVE-2018-0645, CVE-2018-0646, CVE-2018-0647, CVE-2018-0648, CVE-2018-0649, CVE-2018-0650, CVE-2018-0651, CVE-2018-0652, CVE-2018-0653, CVE-2018-0654, CVE-2018-0655, CVE-2018-0656, CVE-2018-0657, CVE-2018-0658, CVE-2018-0659, CVE-2018-0660, CVE-2018-0661, CVE-2018-0662, CVE-2018-0663, CVE-2018-0664, CVE-2018-0665, CVE-2018-0666, CVE-2018-0667, CVE-2018-0668, CVE-2018-0669, CVE-2018-0670, CVE-2018-0671, CVE-2018-0672, CVE-2018-0673, CVE-2018-0674, CVE-2018-0675, CVE-2018-0676, CVE-2018-0677, CVE-2018-0678, CVE-2018-0679, CVE-2018-0680, CVE-2018-0681, CVE-2018-0682, CVE-2018-0683, CVE-2018-0684, CVE-2018-0685, CVE-2018-0686, CVE-2018-0687, CVE-2018-0688, CVE-2018-0689, CVE-2018-0690, CVE-2018-0691, CVE-2018-0692, CVE-2018-0693, CVE-2018-0694, CVE-2018-0695, CVE-2018-0696, CVE-2018-0697, CVE-2018-0698, CVE-2018-0699, CVE-2018-0700, CVE-2018-0701, CVE-2018-0702, CVE-2018-0703, CVE-2018-0704, CVE-2018-0705, CVE-2018-0706, CVE-2018-0707, CVE-2018-0708, CVE-2018-0709, CVE-2018-0710, CVE-2018-0711, CVE-2018-0712, CVE-2018-0713, CVE-2018-0714, CVE-2018-0715, CVE-2018-0716, CVE-2018-0717, CVE-2018-0718, CVE-2018-0719, CVE-2018-0720, CVE-2018-0721, CVE-2018-0722, CVE-2018-0723, CVE-2018-0724, CVE-2018-0725, CVE-2018-0726, CVE-2018-0727, CVE-2018-0728, CVE-2018-0729, CVE-2018-0730, CVE-2018-0731, CVE-2018-0732, CVE-2018-0733, CVE-2018-0734, CVE-2018-0735, CVE-2018-0736, CVE-2018-0737, CVE-2018-0738, CVE-2018-0739, CVE-2018-0740, CVE-2018-0741, CVE-2018-0742, CVE-2018-0743, CVE-2018-0744, CVE-2018-0745, CVE-2018-0746, CVE-2018-0747, CVE-2018-0748, CVE-2018-0749, CVE-2018-0750, CVE-2018-0751, CVE-2018-0752, CVE-2018-0753, CVE-2018-0754, CVE-2018-0755, CVE-2018-0756, CVE-2018-0757, CVE-2018-0758, CVE-2018-0759, CVE-2018-0760, CVE-2018-0761, CVE-2018-0762, CVE-2018-0763, CVE-2018-0764, CVE-2018-0765, CVE-2018-0766, CVE-2018-0767, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0771, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, CVE-2018-0779, CVE-2018-0780, CVE-2018-0781, CVE-2018-0782, CVE-2018-0783, CVE-2018-0784, CVE-2018-0785, CVE-2018-0786, CVE-2018-0787, CVE-2018-0788, CVE-2018-0789, CVE-2018-0790, CVE-2018-0791, CVE-2018-0792, CVE-2018-0793, CVE-2018-0794, CVE-2018-0795, CVE-2018-0796, CVE-2018-0797, CVE-2018-0798, CVE-2018-0799, CVE-2018-0800, CVE-2018-0801, CVE-2018-0802, CVE-2018-0803, CVE-2018-0804, CVE-2018-0805, CVE-2018-0806, CVE-2018-0807, CVE-2018-0808, CVE-2018-0809, CVE-2018-0810, CVE-2018-0811, CVE-2018-0812, CVE-2018-0813, CVE-2018-0814, CVE-2018-0815, CVE-2018-0816, CVE-2018-0817, CVE-2018-0818, CVE-2018-0819, CVE-2018-0820, CVE-2018-0821, CVE-2018-0822, CVE-2018-0823, CVE-2018-0824, CVE-2018-0825, CVE-2018-0826, CVE-2018-0827, CVE-2018-0828, CVE-2018-0829, CVE-2018-0830, CVE-2018-0831, CVE-2018-0832, CVE-2018-0833, CVE-2018-0834, CVE-2018-0835, CVE-2018-0836, CVE-2018-0837, CVE-2018-0838, CVE-2018-0839, CVE-2018-0840, CVE-2018-0841, CVE-2018-0842, CVE-2018-0843, CVE-2018-0844, CVE-2018-0845, CVE-2018-0846, CVE-2018-0847, CVE-2018-0848, CVE-2018-0849, CVE-2018-0850, CVE-2018-0851, CVE-2018-0852, CVE-2018-0853, CVE-2018-0854, CVE-2018-0855, CVE-2018-0856, CVE-2018-0857, CVE-2018-0858, CVE-2018-0859, CVE-2018-0860, CVE-2018-0861, CVE-2018-0862, CVE-2018-0863, CVE-2018-0864, CVE-2018-0865, CVE-2018-0866, CVE-2018-0867, CVE-2018-0868, CVE-2018-0869, CVE-2018-0870, CVE-2018-0871, CVE-2018-0872, CVE-2018-0873, CVE-2018-0874, CVE-2018-0875, CVE-2018-0876, CVE-2018-0877, CVE-2018-0878, CVE-2018-0879, CVE-2018-0880, CVE-2018-0881, CVE-2018-0882, CVE-2018-0883, CVE-2018-0884, CVE-2018-0885, CVE-2018-0886, CVE-2018-0887, CVE-2018-0888, CVE-2018-0889, CVE-2018-0890, CVE-2018-0891, CVE-2018-0892, CVE-2018-0893, CVE-2018-0894, CVE-2018-0895, CVE-2018-0896, CVE-2018-0897, CVE-2018-0898, CVE-2018-0899, CVE-2018-0900, CVE-2018-0901, CVE-2018-0902, CVE-2018-0903, CVE-2018-0904, CVE-2018-0905, CVE-2018-0906, CVE-2018-0907, CVE-2018-0908, CVE-2018-0909, CVE-2018-0910, CVE-2018-0911, CVE-2018-0912, CVE-2018-0913, CVE-2018-0914, CVE-2018-0915, CVE-2018-0916, CVE-2018-0917, CVE-2018-0918, CVE-2018-0919, CVE-2018-0920, CVE-2018-0921, CVE-2018-0922, CVE-2018-0923, CVE-2018-0924, CVE-2018-0925, CVE-2018-0926, CVE-2018-0927, CVE-2018-0928, CVE-2018-0929, CVE-2018-0930, CVE-2018-0931, CVE-2018-0932, CVE-2018-0933, CVE-2018-0934, CVE-2018-0935, CVE-2018-0936, CVE-2018-0937, CVE-2018-0938, CVE-2018-0939, CVE-2018-0940, CVE-2018-0941, CVE-2018-0942, CVE-2018-0943, CVE-2018-0944, CVE-2018-0945, CVE-2018-0946, CVE-2018-0947, CVE-2018-0948, CVE-2018-0949, CVE-2018-0950, CVE-2018-0951, CVE-2018-0952, CVE-2018-0953, CVE-2018-0954, CVE-2018-0955, CVE-2018-0956, CVE-2018-0957, CVE-2018-0958, CVE-2018-0959, CVE-2018-0960, CVE-2018-0961, CVE-2018-0962, CVE-2018-0963, CVE-2018-0964, CVE-2018-0965, CVE-2018-0966, CVE-2018-0967, CVE-2018-0968, CVE-2018-0969, CVE-2018-0970, CVE-2018-0971, CVE-2018-0972, CVE-2018-0973, CVE-2018-0974, CVE-2018-0975, CVE-2018-0976, CVE-2018-0977, CVE-2018-0978, CVE-2018-0979, CVE-2018-0980, CVE-2018-0981, CVE-2018-0982, CVE-2018-0983, CVE-2018-0984, CVE-2018-0985, CVE-2018-0986, CVE-2018-0987, CVE-2018-0988, CVE-2018-0989, CVE-2018-0990, CVE-2018-0991, CVE-2018-0992, CVE-2018-0993, CVE-2018-0994, CVE-2018-0995, CVE-2018-0996, CVE-2018-0997, CVE-2018-0998, CVE-2018-0999, CVE-2018-1000, CVE-2018-1001, CVE-2018-1002, CVE-2018-1003, CVE-2018-1004, CVE-2018-1005, CVE-2018-1006, CVE-2018-1007, CVE-2018-1008, CVE-2018-1009, CVE-2018-1010, CVE-2018-1011, CVE-2018-1012, CVE-2018-1013, CVE-2018-1014, CVE-2018-1015, CVE-2018-1016, CVE-2018-1017, CVE-2018-1018, CVE-2018-1019, CVE-2018-1020, CVE-2018-1021, CVE-2018-1022, CVE-2018-1023, CVE-2018-1024, CVE-2018-1025, CVE-2018-1026, CVE-2018-1027, CVE-2018-1028, CVE-2018-1029, CVE-2018-1030, CVE-2018-1031, CVE-2018-1032, CVE-2018-1033, CVE-2018-1034, CVE-2018-1035, CVE-2018-1036, CVE-2018-1037, CVE-2018-1038, CVE-2018-1039, CVE-2018-1040, CVE-2018-1041, CVE-2018-1042, CVE-2018-1043, CVE-2018-1044, CVE-2018-1045, CVE-2018-1046, CVE-2018-1047, CVE-2018-1048, CVE-2018-1049, CVE-2018-1050, CVE-2018-1051, CVE-2018-1052, CVE-2018-1053, CVE-2018-1054, CVE-2018-1055, CVE-2018-1056, CVE-2018-1057, CVE-2018-1058, CVE-2018-1059, CVE-2018-1060, CVE-2018-1061, CVE-2018-1062, CVE-2018-1063, CVE-2018-1064, CVE-2018-1065, CVE-2018-1066, CVE-2018-1067, CVE-2018-1068, CVE-2018-1069, CVE-2018-1070, CVE-2018-1071, CVE-2018-1072, CVE-2018-1073, CVE-2018-1074, CVE-2018-1075, CVE-2018-1076, CVE-2018-1077, CVE-2018-1078, CVE-2018-1079, CVE-2018-1080, CVE-2018-1081, CVE-2018-1082, CVE-2018-1083, CVE-2018-1084, CVE-2018-1085, CVE-2018-1086, CVE-2018-1087, CVE-2018-1088, CVE-201

## Функционирование ФинЦЕРТ: Что ещё получает участник обмена

оперативное информирование, реагирование и консультации участника по обращениям в ФинЦЕРТ;

проведение анализа вредоносных файлов;

получение уведомлений об обнаружении подозрительной активности при взаимодействии Интернет с сетями/ресурсами КО (участника обмена);

оперативное реагирование при выявлении хищения у КО или клиента КО;

консультация сотрудников ФинЦЕРТ по предотвращению кибератак/хищений (с применением ИКТ) и/или минимизации ущерба;

возможное участие сотрудников ФинЦЕРТ в анализе серьезных инцидентов (крупного хищения, атаки и т.п.);

поиск, анализ и предотвращение функционирования (инициация разделегирования/ блокировки) мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере и сайтов, распространяющих вредоносное программное обеспечение;

мониторинг информационных атак на КО (участника обмена) в СМИ и соцсетях;

и т.д.

# Динамика развития АСОИ ФинЦЕРТ

- Обмен с участниками через защищенный портал +ЛК и e-mail (получение информации в форматах XLSx и JSON)
- Автоматизация ключевых процессов
- Автоматическое взаимодействие с ГосСОПКА;
- Реализация функционала «Фид-антифрода» для Участников обмена

До  
01.07.2018

- Обмен с участниками по e-mail (получение информации в формате XLSx )
- Локальная автоматизация работы экспертов
- Функционирование базовых процессов

2018-  
2019 (2  
кв.)

- Обмен с участниками через защищенный портал, e-mail (получение информации в форматах XLSx и JSON) и API
- Предоставление Участникам сервиса по проверке ВПО
- Автоматическое взаимодействие с ГосСОПКА
- Поддержка функционала для реализации 167-ФЗ в полном объеме
- Возможность взаимодействия с иностранными участниками

**Настоящее  
время**

**Создана 1-я**



# Порядок подключения к АСОИ ФинЦЕРТ

**Получение комплекта участника**  
[http://cbr.ru/StaticHtml/File/14408/ASOI\\_docs.zip](http://cbr.ru/StaticHtml/File/14408/ASOI_docs.zip)

**Заполнение и отправка в ФинЦЕРТ карточки участника**  
[http://cbr.ru/StaticHtml/File/14406/member\\_card.xlsx](http://cbr.ru/StaticHtml/File/14406/member_card.xlsx)

**Настройка рабочих мест для подключения к АСОИ ФинЦЕРТ (установка и настройка СКЗИ, настройка сетевых параметров подключения и проверка доступа к информационному portalу ФинЦЕРТ**  
<https://portal.fincert.cbr.ru>

**Проверка доступа к Личному кабинету в АСОИ ФинЦЕРТ**  
<https://lk.fincert.cbr.ru>, отправка тестового запроса

**+++!!! Вы подключены к АСОИ ФинЦЕРТ !!! +++**

**Подключение и активация пользователей в ЛК АСОИ ФинЦЕРТ (осуществляется ответственным сотрудником Участника)**



Получение и проверка заполнения карточки участника

Регистрация Участника и ответственного в АСОИ ФинЦЕРТ

Отправка ответственному первичного пароля для ЛК в АСОИ ФинЦЕРТ

Не более 7 рабочих дней



## Подключение к АСОИ ФинЦЕРТ. Карточка участника



|                                                            |  |
|------------------------------------------------------------|--|
| Название участника информационного обмена (полное)         |  |
| Название участника информационного обмена (сокращенное)    |  |
| Город (головной офис)                                      |  |
| Регистрационный номер поднадзорной организации (если есть) |  |
| Групповой почтовый адрес для информационного обмена        |  |
| Внешние IP адреса участника информационного обмена         |  |
| Оператор связи (основной, резервный)                       |  |

|                                                                                                                                                                   |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Состав используемого <b>критичного</b> программного/аппаратного обеспечения с версиями (требуется для адресного направления информации по выявленным уязвимостям) |  |
| ОС                                                                                                                                                                |  |
| СУБД для АБС, ДБО                                                                                                                                                 |  |
| АБС                                                                                                                                                               |  |
| ДБО                                                                                                                                                               |  |
| Антивирус                                                                                                                                                         |  |
| МЭ                                                                                                                                                                |  |
| POS терминалы                                                                                                                                                     |  |
| Банкоматы                                                                                                                                                         |  |
| Прочее (на усмотрение участника)                                                                                                                                  |  |

| Контактные данные участника информационного обмена (для оперативной связи в случае выявления целевой атаки на организацию или иных чрезвычайных обстоятельствах) |                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                  | Контактные данные                                                                                                                                                                                                         |
| Куратор информационного взаимодействия из числа руководителей организации                                                                                        | <div>ФИО</div> <div>Должность (с указанием подразделения)</div> <div>Рабочий телефон ( формат: 7(код города)xxx xx xx)</div> <div>Мобильный телефон (формат: 7(код оператора)xxx xx xx)</div> <div>Контактный email</div> |
| Ответственный за информационный обмен и управление пользователями Участника (подключение к АСОИ ФинЦЕРТ)                                                         |                                                                                                                                                                                                                           |
| Зам. ответственного за информационный обмен и управление пользователями Участника (подключение к АСОИ ФинЦЕРТ)                                                   |                                                                                                                                                                                                                           |
| Начальник службы информационной безопасности                                                                                                                     |                                                                                                                                                                                                                           |
| Замещающий сотрудник службы информационной безопасности                                                                                                          |                                                                                                                                                                                                                           |
| Начальник службы мониторинга (Анти-фрод)                                                                                                                         |                                                                                                                                                                                                                           |
| Замещающий сотрудник службы мониторинга (Анти-фрод)                                                                                                              |                                                                                                                                                                                                                           |
| IT                                                                                                                                                               |                                                                                                                                                                                                                           |
| Подразделение, обрабатывающее риски                                                                                                                              |                                                                                                                                                                                                                           |

## Подключение к АСОИ ФинЦЕРТ.

1. Основные документы:
  - *Регламент подключения участников информационного обмена к АСОИ ФинЦЕРТ;*
  - *Руководство Участника по работе с АСОИ ФинЦЕРТ.*
2. «Карточка участника» отправляется на электронный адрес [info\\_fincert@cbr.ru](mailto:info_fincert@cbr.ru) с пометкой **«Информационное взаимодействие»**.
3. Информационный портал ФинЦЕРТ - <https://portal.fincert.cbr.ru>
4. Личный кабинет участника в АСОИ ФинЦЕРТ - <https://lk.fincert.cbr.ru>
5. В случае возникновения ошибок необходимо подготовить подробное описание (версия ОС, версия браузера, версия СКЗИ, описание ошибки, снимки экрана, на которых видна ошибка) и направить на адрес электронной почты [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).
6. В случае возникновения вопросов по подключению и использованию АСОИ ФинЦЕРТ - вопросы направлять на адрес [info\\_fincert@cbr.ru](mailto:info_fincert@cbr.ru) и [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).



# Единая система антифрод и 167-ФЗ

БАНК РОССИИ



1. Совпадение информации о получателе средств с информацией о получателе средств по переводам денежных средств без согласия клиента, полученной из базы данных о случаях и попытках осуществления перевода денежных средств без согласия клиента, формируемой Банком России в соответствии с частью 5 статьи 27 ФЗ-161 от 27.06.2011. (далее база данных).
2. Совпадение информации о параметрах устройств, с использованием которых был осуществлен доступ к автоматизированной системе, ПО с целью осуществления перевода денежных средств, с информацией о параметрах устройств, с использованием которых был осуществлен доступ к АС, ПО с целью осуществления перевода денежных средств без согласия клиента, полученной из базы данных.
3. Несоответствие характера, и (или) параметров, и (или) объема проводимой операции (время (дни) осуществления операции, место осуществления операции, устройство, с использованием которого осуществляется операция и параметры его использования, сумма осуществления операции, периодичность (частота) осуществления операций, получатель средств), операциям, обычно совершаемым клиентом оператора по переводу денежных средств (осуществляемой клиентом деятельности)



## Действия при выявлении операций, соответствующих признакам операций без согласия

Клиент не  
прошел  
идентификац  
ию

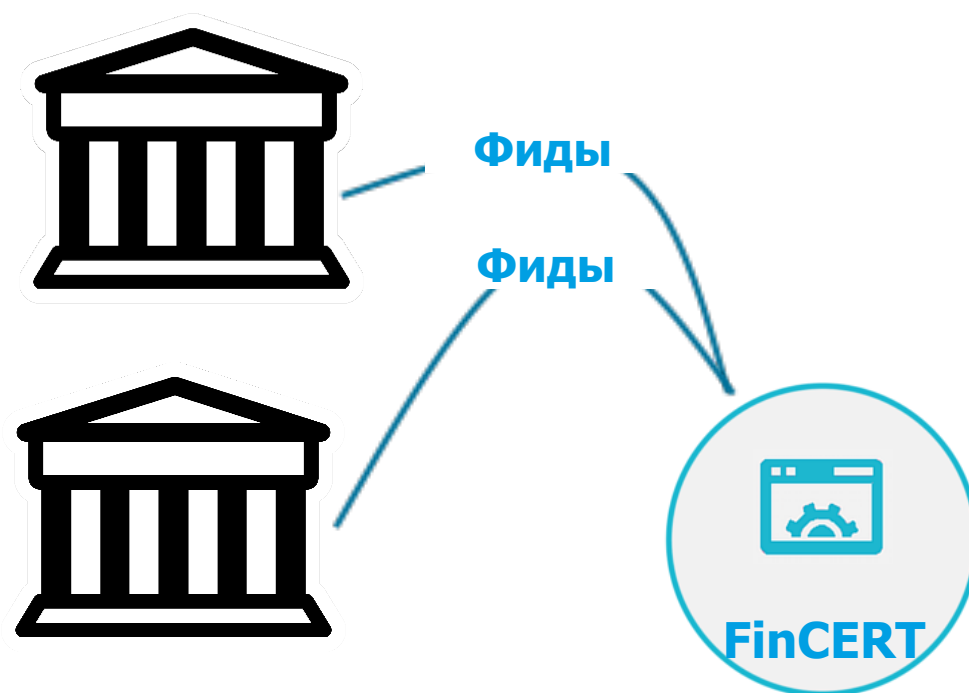
# База операций без согласия

| № | Поле                                                                   |
|---|------------------------------------------------------------------------|
| 1 | Информация о плательщике                                               |
| 2 | Информация об операции                                                 |
| 3 | Информация о получателе                                                |
| 4 | Параметры устройства, с которого осуществлена транзакция (при наличии) |
| 5 | Статусы и допстатусы (флаги)                                           |

# База операций без согласия. Наполнение



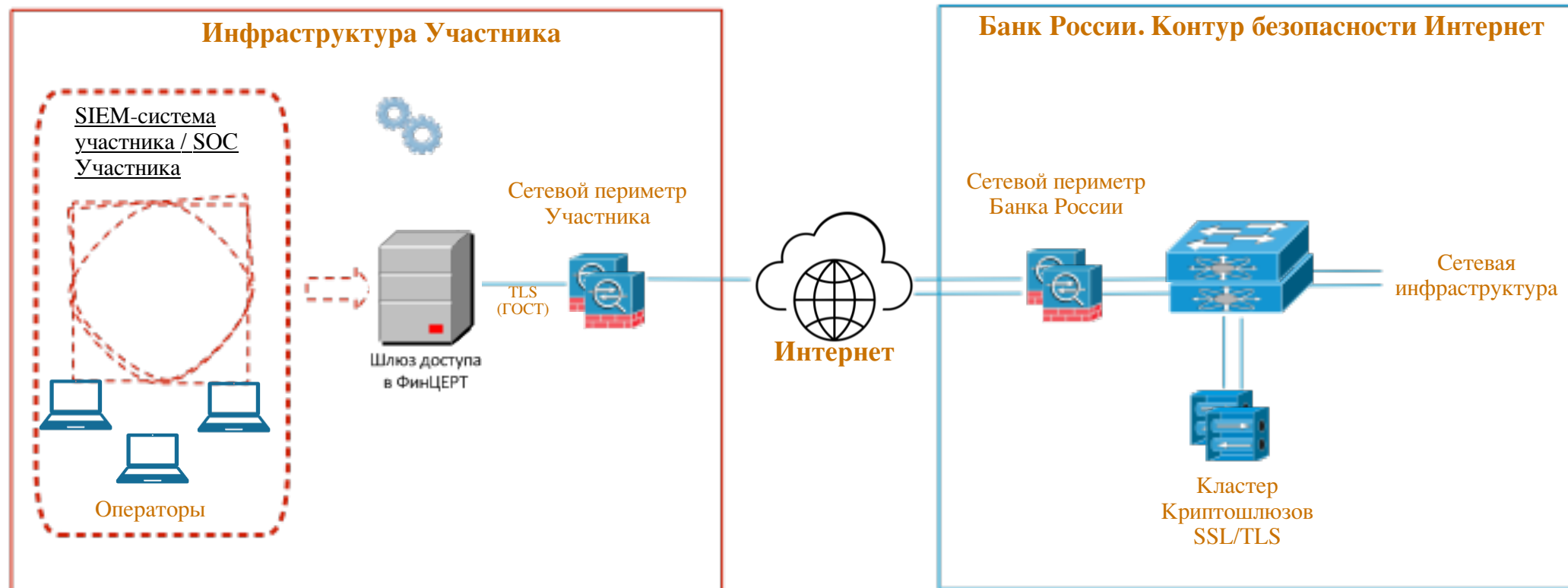
# База операций без согласия. Распространение



Банк России  
распространяет фиды,  
которые содержат:

- Значимый реквизит
  - Дата последней записи в БД
  - Значимые реквизиты актуальной записи в БД
  - Количество записей
  - Номер счета + БИК
  - Номер карты
  - Номер телефона
  - Номер кошелька
  - ИНН
  - IP устройства
  - IMSI
  - IMEI
  - Хэш от номера паспорта
  - Хэш от номера СНИЛС
- Группа 1
- Группа 2

# Расширение возможностей взаимодействия с Участниками (2-я очередь)



- Шлюз автоматической интеграции SIEM-систем / SOC Участника с АСОИ ФинЦЕРТ:
- MaxPatrol SIEM (Positive Technologies)
- ArcSight (MicroFocus)
- QRadar (IBM)
- Автоматический прием инцидентов и дополнительной информации, регистрация их в АСОИ ФинЦЕРТ и запуск процессов реагирования

