АСОИ ФинЦЕРТ – платформа Банка России по обработке инцидентов

БАНК РОССИИ
ФИНЦЕРТ

План доклада-презентации:

План доклада-презентации:

- Предпосылки создания АСОИ ФинЦЕРТ
- Цели и задачи создания АСОИ ФинЦЕРТ.
  Основные прикладные процессы АСОИ ФинЦЕРТ
- Функционирование АСОИ ФинЦЕРТ: что получает участник информационного обмена
- Порядок подключения к АСОИ ФинЦЕРТ
- Личный кабинет АСОИ ФинЦЕРТ

Предпосылки создания АСОИ ФинЦЕРТ

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.

Цели и задачи создания АСОИ ФинЦЕРТ

Создание единого механизма автоматизированного защищенного доверенного взаимодействия Банка России и Участников

Технологическая поддержка процессов взаимодействия с Участников и ФинЦЕРТ

Оперативное информирование Участников об актуальных угрозах ИБ в КФС

- 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

Основные прикладные процессы АСОИ ФинЦЕРТ

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

Функционирование АСОИ ФинЦЕРТ: Что получает участник обмена

Бюллетени ФинЦЕРТ:

О рассылках вирусов (ВПО) в КФС

Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксированы факты распространения вредоносного программного обеспечения. Предположительно, осуществляется массовая атака на организации кредитно-финансовой сферы с использованием ПО «Cobalt Strike» или аналогичного по функциональным возможностям.

2. Основные индикаторы компрометации

№	Тип IOC	Список
1	URL-адреса и IP-адреса, к которым производятся обращения	dieboldnixdorf[.]us api.asus.org[.]kz documents.total-cloud[.]biz 62.76.42[.]78 31.148.220[.]105 185.223.95[.]112
2	Адреса и домены отправителей писем	@dieboldnixdorf[.]us 193.180.164[.]40

Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусными средствами различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей организации антивирусного средства.

Обращаем внимание на то, что использование авторами рассылки ВПО иных имён файлов, кроме указанных в настоящем бюллетене, **не исключено**.

1) «Security_protocol.doc»

MD5	92F1BB5AA4A1C6C8AC81CBFDC2B3698A
SHA1	BD1E815DD492BE3FF0EC54351FE61CE1B0E2A5AF
SHA256	E566DB9E491FDA7A5D28FFE9019BE64B4D9BC75014BBE189A9DCB9D987856558
Размер файла (байт)	83968

Email: fincert@cbr.ru

Об атаках

FinCERT Банка России

PC-V:EN-WannaCry-20170514-01

Рассылка информации о возможной угрозе – шифровальщик WannaCry

1. Краткое описание угрозы

12.05.2017 зафиксированы случаи массового заражения шифровальщиком-вымогателем WannaCry с последующим требованием выкупа в BTC (биткойн), эквивалентным от 300 до 600 USD.

Отличительными особенностями вредоносного программного обеспечения являются:

- Использование уязвимости протоколов SMB v.1, SMB v.2 «EternalBlue» (из архива Shadowbrokers). SMB v.3 по предварительным данным не подвержена указанной уязвимости (данная версия используется, начиная с ОС Windows 8 / Windows Server 2012);
- Функционал сетевого червя: производится поиск соседних устройств в той же локальной сети или смежных сетях, куда имеет доступ зараженное устройство и заражает, в свою очередь, их. Этим объясняется лавинообразное распространение заражений.

При заражении шифруются файлы баз данных, документы и прочие «чувствительные» файлы. Файл для шифрования выбирается по его расширению.

По состоянию на 14.05.2017 детектируется большинством антивирусных решений, но обращаем внимание, что даже в этом случае часть файлов может оказаться зашифрованными.

По состоянию на 14.05.2017 средства расшифровки отсутствуют.

2. Основные меры противодействия (превентивные)

1. На серверах / пользовательских АРМ: организовать резервирование всех важных файлов с **использованием сторонних средств резервирования** (отличных от «теневых копий» документов Windows и средства восстановления Windows, т.к. данные резервные копии могут быть уничтожены в процессе работы ВПО), обязательно включив в список файлы со следующими расширениями: .der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv,

Email: fincert@cbr.ru

Функционирование АСОИ ФинЦЕРТ: Что получает участник обмена

Информационные бюллетени

ИР-20180609

РС– ОТН:BN–BACKSWAP–20180609–01:i

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 Nemucod. 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. 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@cbr.ru

Предупреждения об уязвимостях

Предупреждение! RCE уязвимости некоторых устройств Cisco!

1. Краткое описание угрозы

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

Атакующие настраивают бот-сети на сканирование устройств с открытыми портами TCP:4786 (уязвимость в Cisco IOS Smart Install, CVE-2018-0171, CVSS: 9.8) и UDP:18999 (уязвимость в Adaptive QoS for DMVPN сервисе Cisco, CVE-2018-0151, CVSS: 9.8). Обе эти уязвимости эксплуатируются путем некорректной проверки получаемых устройством пакетов.

Успешное эксплуатирование указанных уязвимостей позволяет, как минимум, изменить файл конфигурации, перезагрузить оборудование, выполнить команды в CLI с высоким уровнем привилегий, а также возможно загрузить «свой» образ IOS.

Предполагается, что для поиска уязвимых устройств используется поисковик Shodan, а также простое сканирование сети.

2. Устройства, на которые следует обратить особое внимание

- Catalyst 4500 Supervisor Engines;
- Catalyst 2975/2960/3560/3650'3750/3850;
- IE 2000/3000/3010/4000/4010/5000;
- NME-16ES-1G-P;
- SM-ES2;
- SM-ES3
- SM-X-ES3

3. Меры противодействия

Основной мерой противодействия является установка патча, выпущенного компанией Cisco 29.03.2018 (hxxps://tools.cisco.com/security/center/viewErp.x?alertId=ERP-66682, подробнее о закрываемых уязвимостях см. информационный бюллетень ФинЦЕРТ ИР-20180330 от 30.03.2018).

В качестве ***временных*** возможно использование следующих мер противодействия:

Для уязвимости CVE-2018-0171:

- Ограничение доступа к порту TCP:4786 с помощью списков доступа (пример ниже)

```
ip access-list extended SMI_HARDENING
permit tcp host <адрес Cisco> host <кому разрешен доступ к Smart Install> eq 4786
deny tcp any any eq 4786
permit ip any any
```

- Отключение vstack ("no vstack" в CLI) (**важно:** команда no vstack **не сохраняется** после перезагрузки на устройствах Catalyst 4500/4550-X (версии 3.9.2E / 15.2 (5)E2), Catalyst 6500 (версии 15.1 (2) SY11,

Email: fincert@cbr.ru

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

До 01.07.2018

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

Настоящее время

Создана 1-я очередь 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

2018-2019 (2 кв.)

2-я очередь АСОИ ФинЦЕРТ

- 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

Порядок подключения к АСОИ ФинЦЕРТ

Получение комплекта участника
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

Настройка рабочих мест для подключения к АСОИ ФинЦЕРТ (установка и настройка СКЗИ, настройка сетевых параметров подключения и проверка доступа к информационному порталу 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 **критичного** 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)	

Подключение к АСОИ ФинЦЕРТ. Карточка 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	ФИО Должность (с указанием подразделения) Рабочий телефон (формат: 7(код города)xxx xx xx) Мобильный телефон (формат: 7(код оператора)xxx xx xx) Контактый email
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	
Платежные технологии	

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 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.
6. В случае возникновения вопросов по подключению и использованию АСОИ ФинЦЕРТ - вопросы направлять на адрес info_fincert@cbr.ru и svc_fincert_support@cbr.ru.

Участники информационного обмена

437 - кредитных организации (КО);

105 - некредитные финансовые организации;

3 - разработчики банковского программного обеспечения;

18 - небанковские кредитные организации;

8 –региональных органа власти;

8 – операторов платежных систем;

6 - операторы связи;

3 - антивирусные компании;

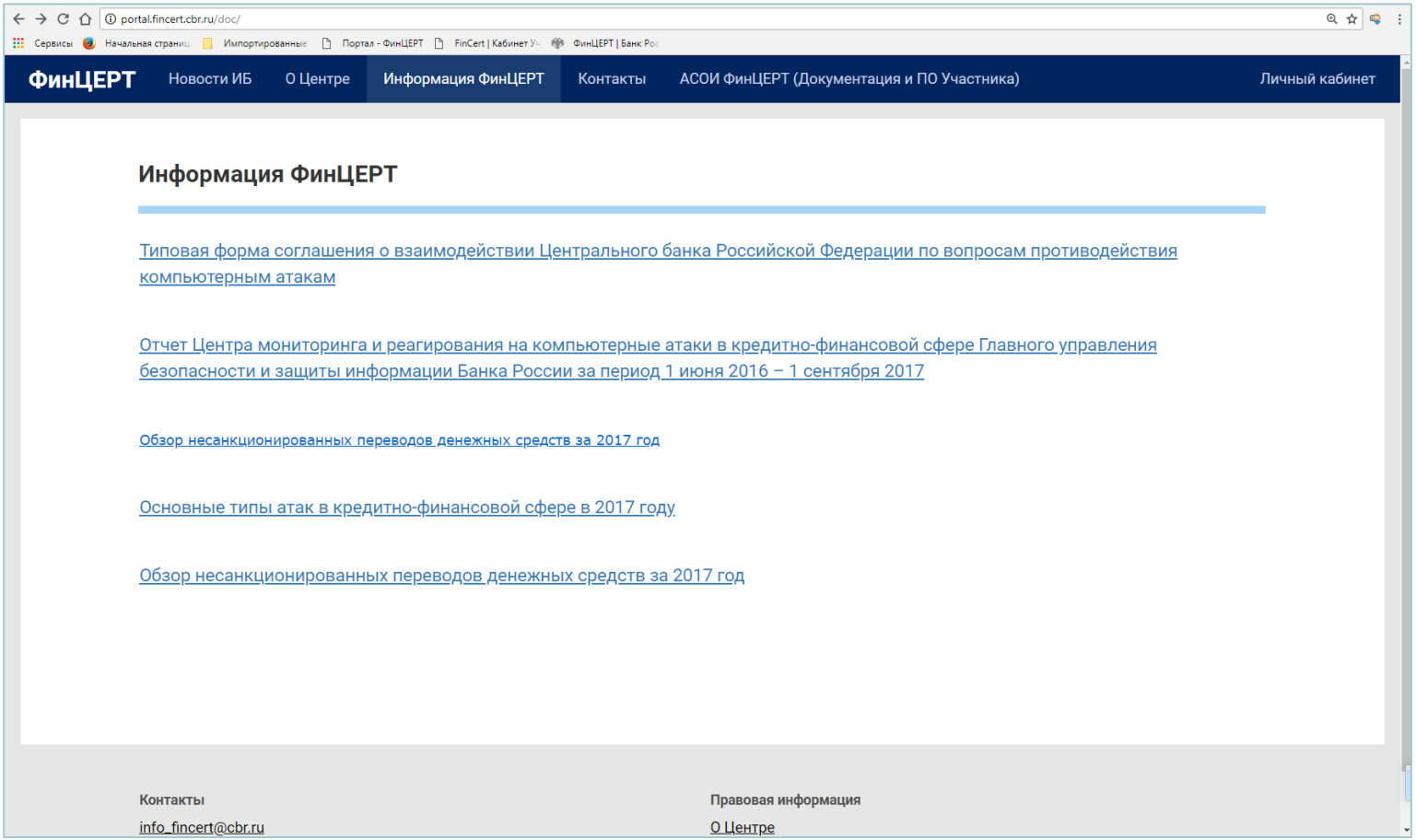
2 - правоохранительные органы;

43 - иные организации.

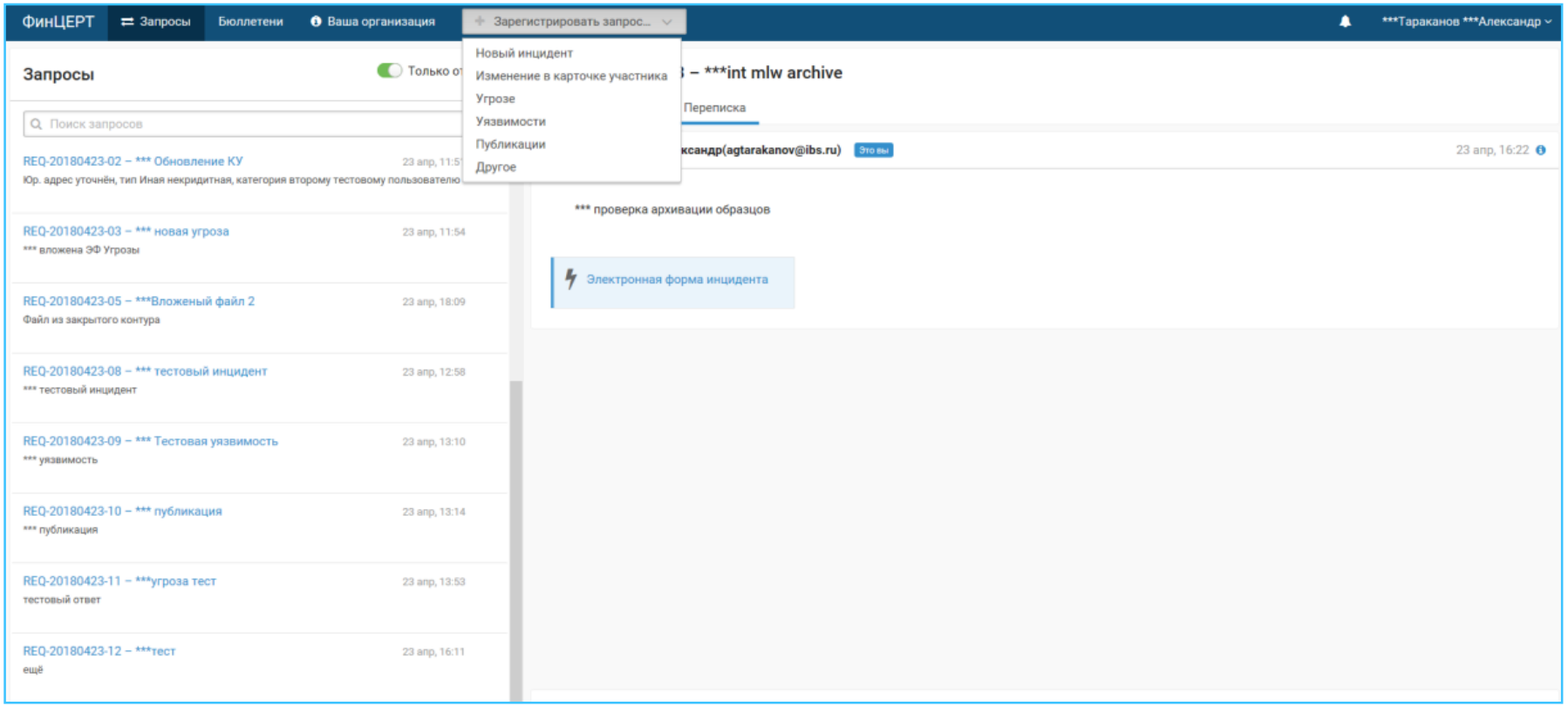
Всего: 633

Подключены к АСОИ ФинЦЕРТ: 194 КО

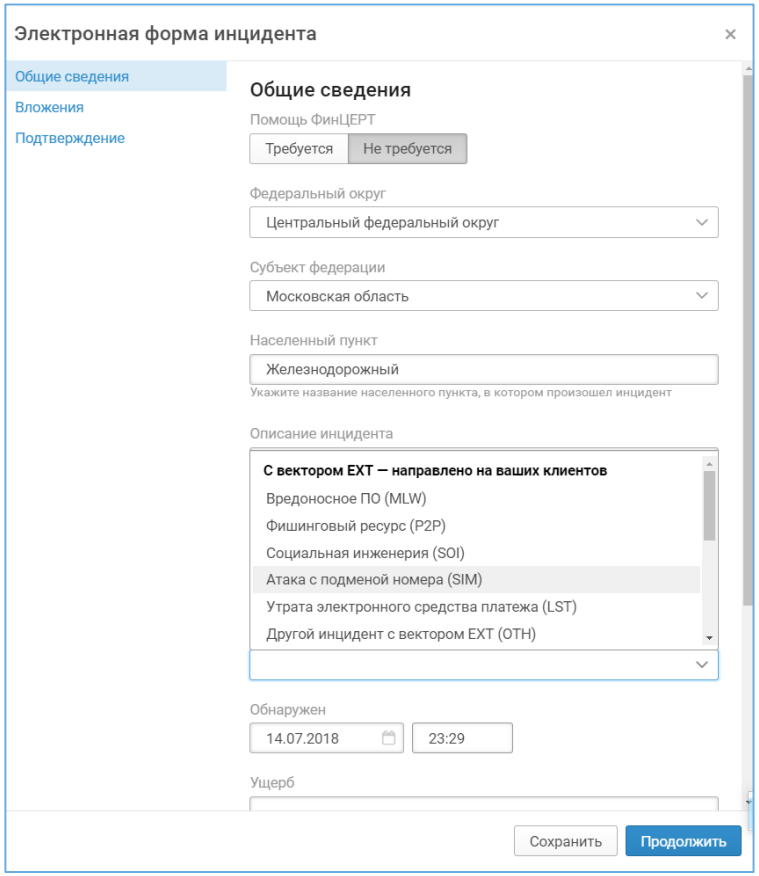
«Работа в АСОИ ФинЦЕРТ» : Портал участника

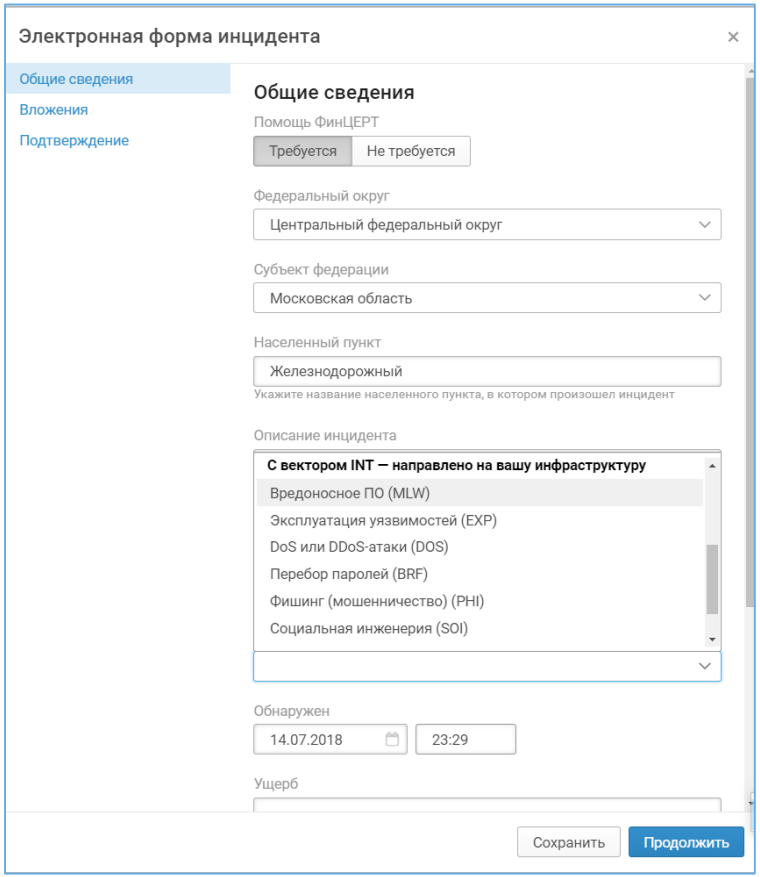


Личный кабинет АСОИ ФинЦЕРТ

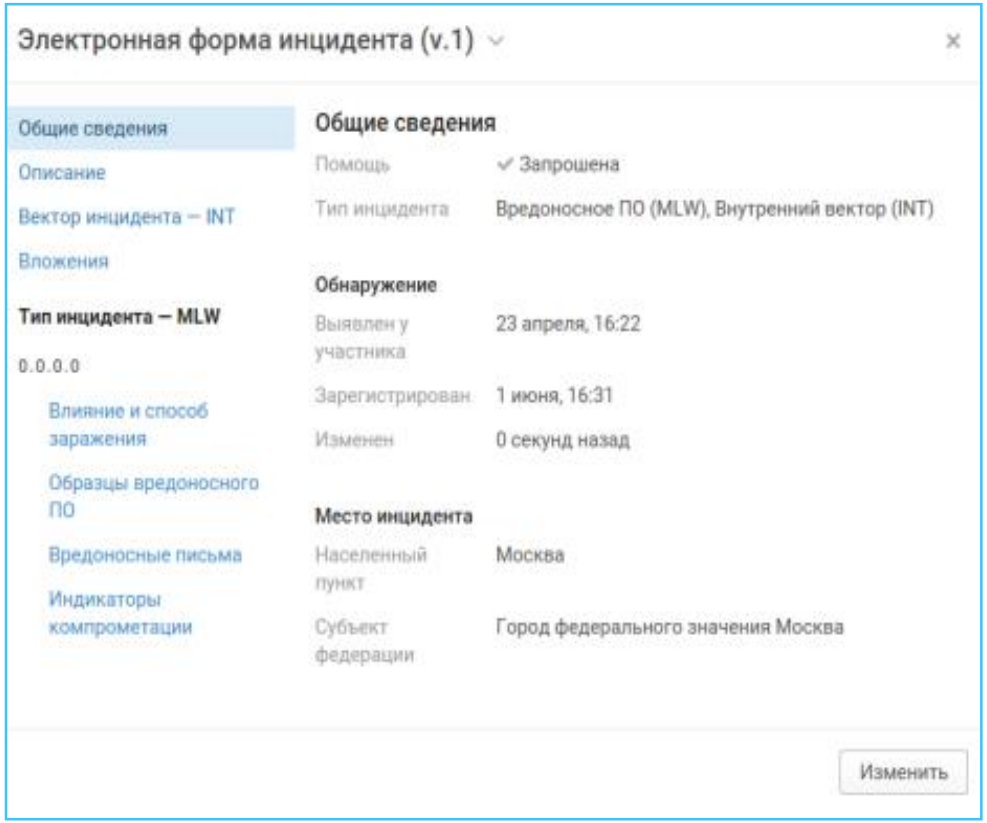


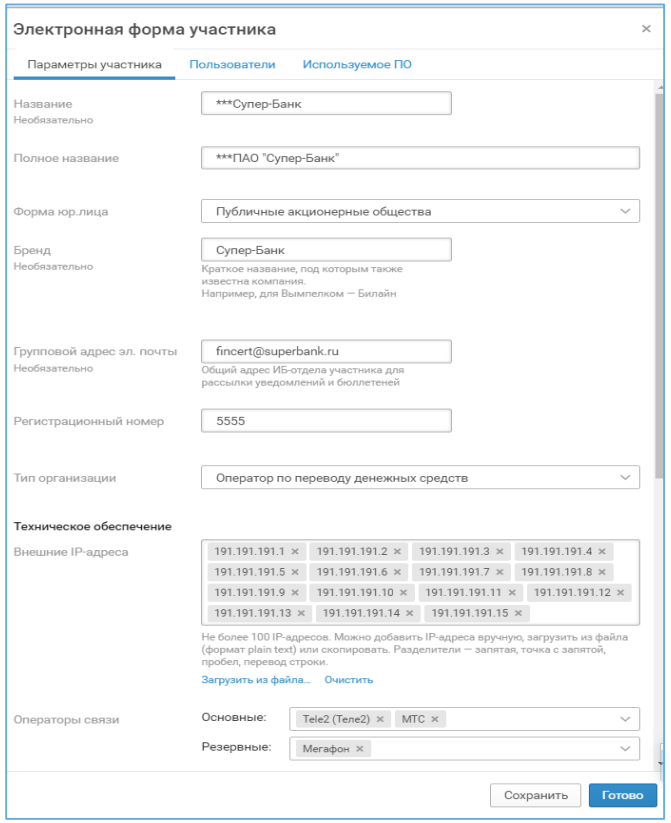
Личный кабинет АСОИ ФинЦЕРТ



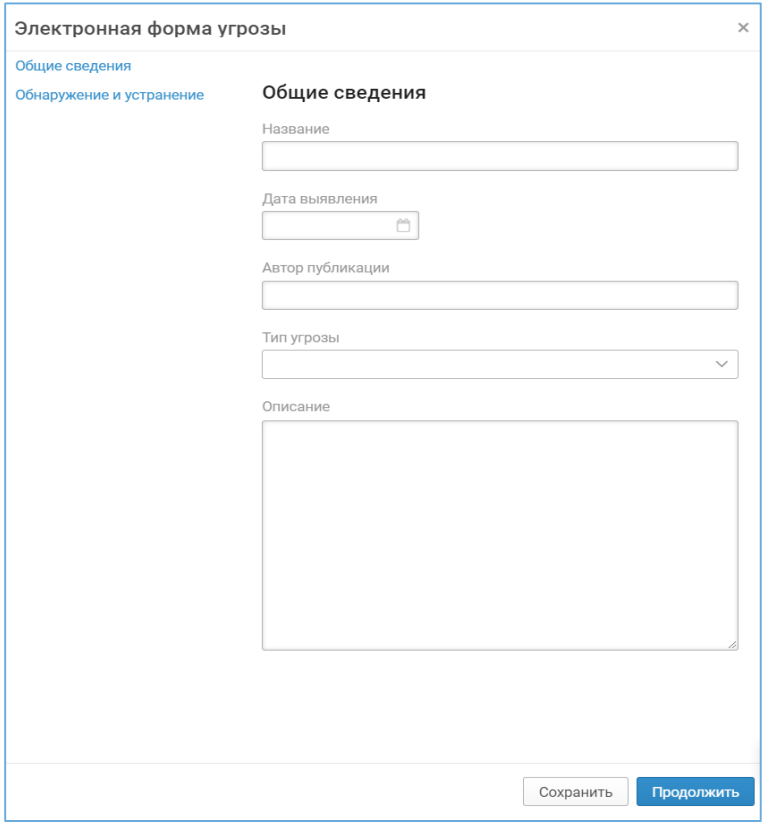


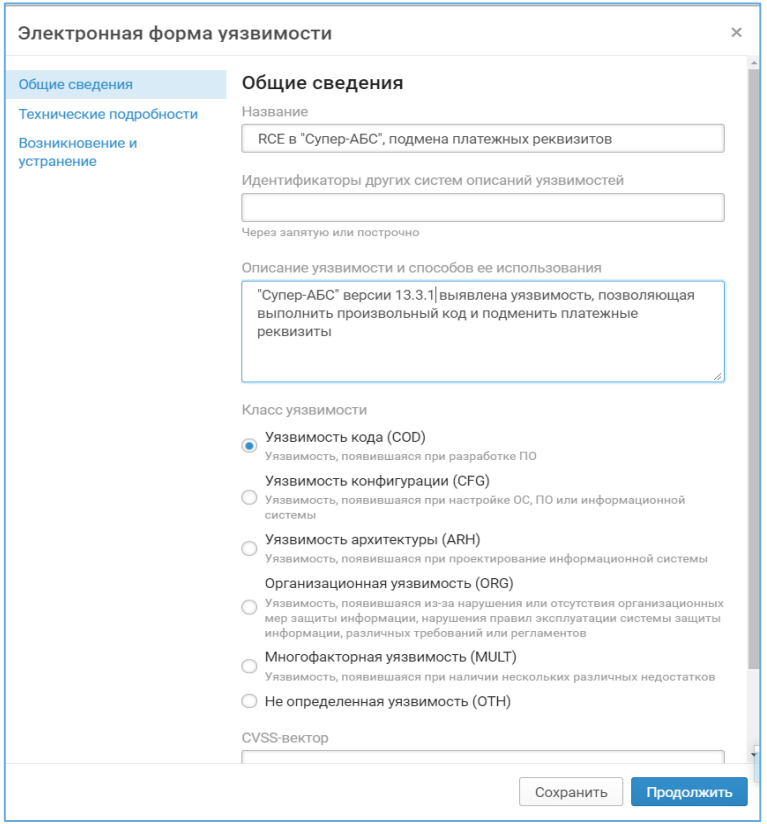
Личный кабинет АСОИ ФинЦЕРТ



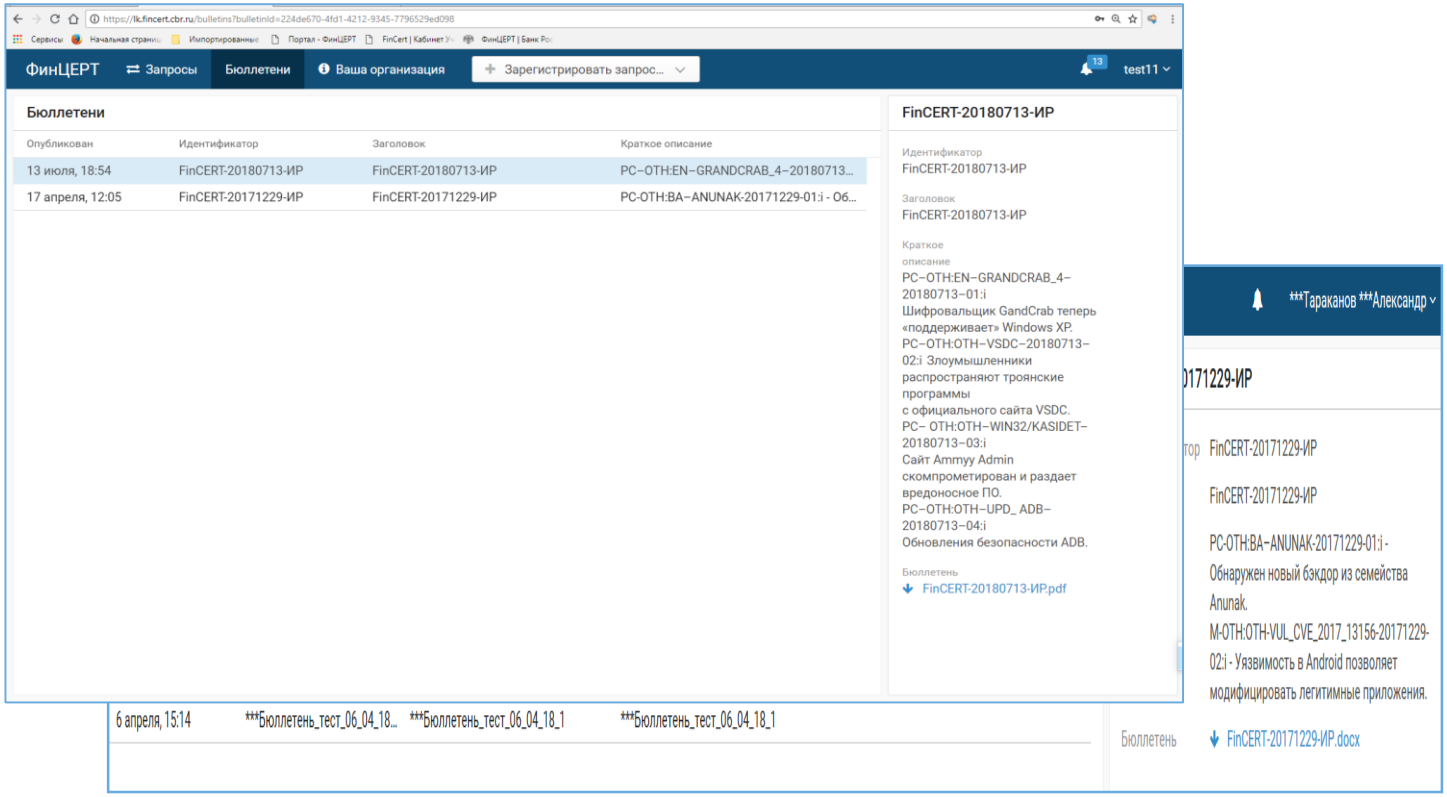


Личный кабинет АСОИ ФинЦЕРТ

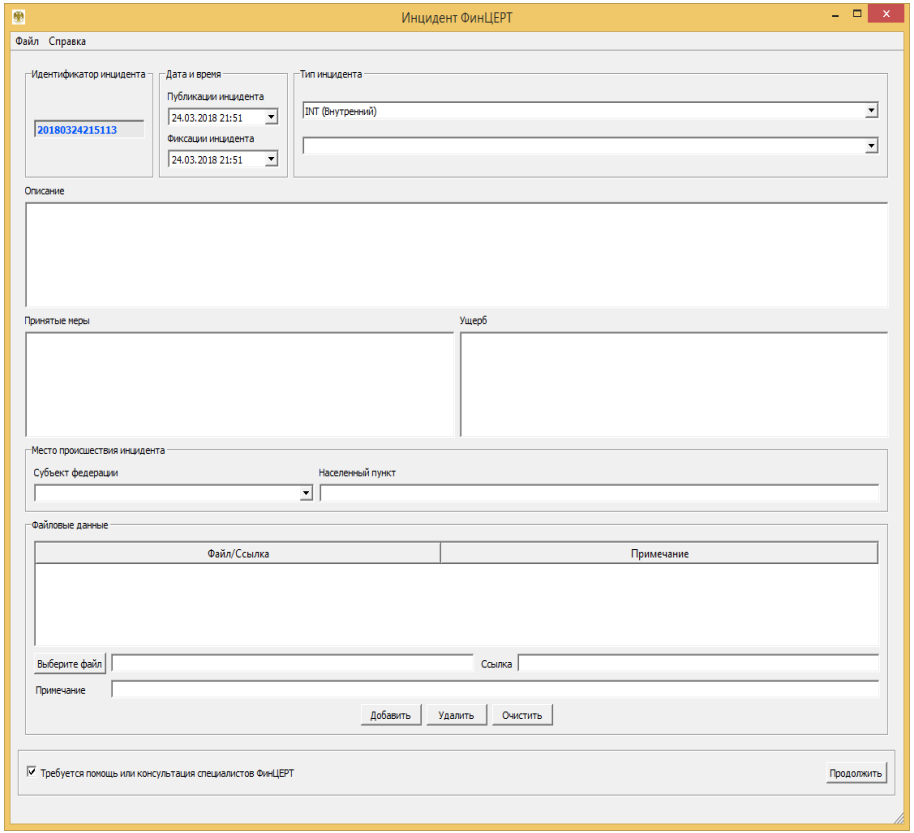


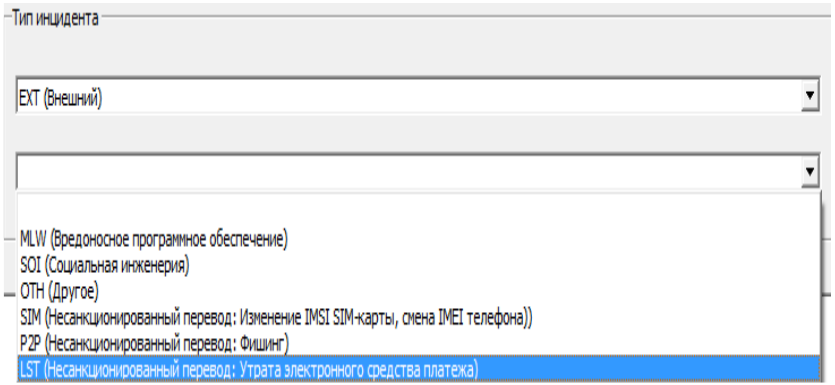


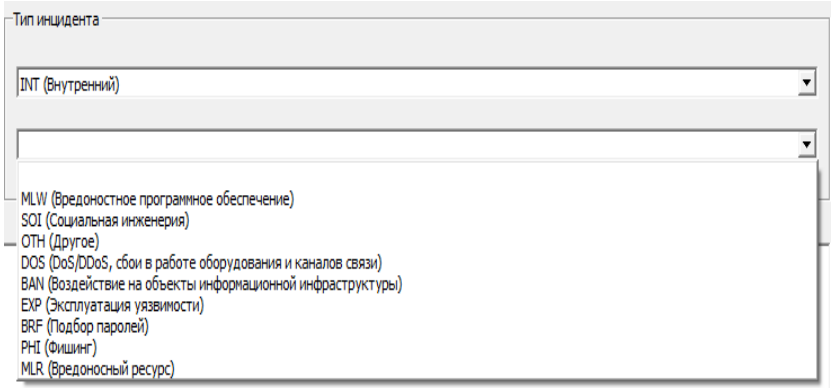
Личный кабинет АСОИ ФинЦЕРТ



Приложение Инцидент ФинЦЕРТ



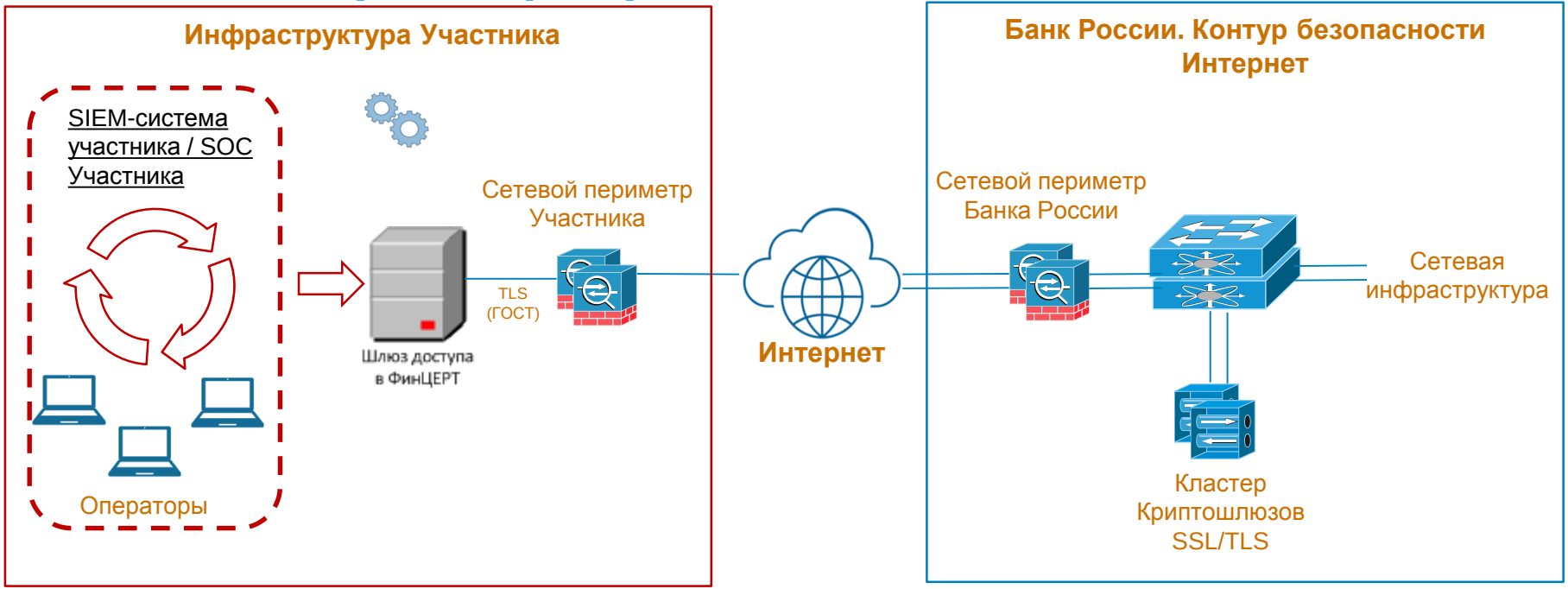




Спасибо за внимание!

БАНК РОССИИ
ФИНЦЕРТ

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