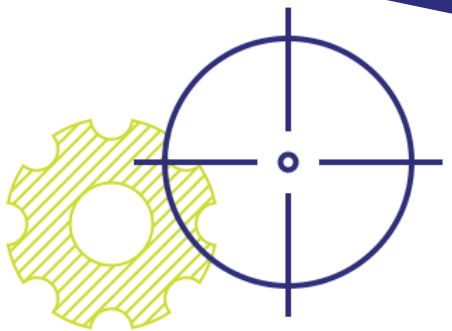
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ



Сценарии автоматизации реагирования на инциденты кибербезопасности

Incident Response Platform (IRP/SOAR)

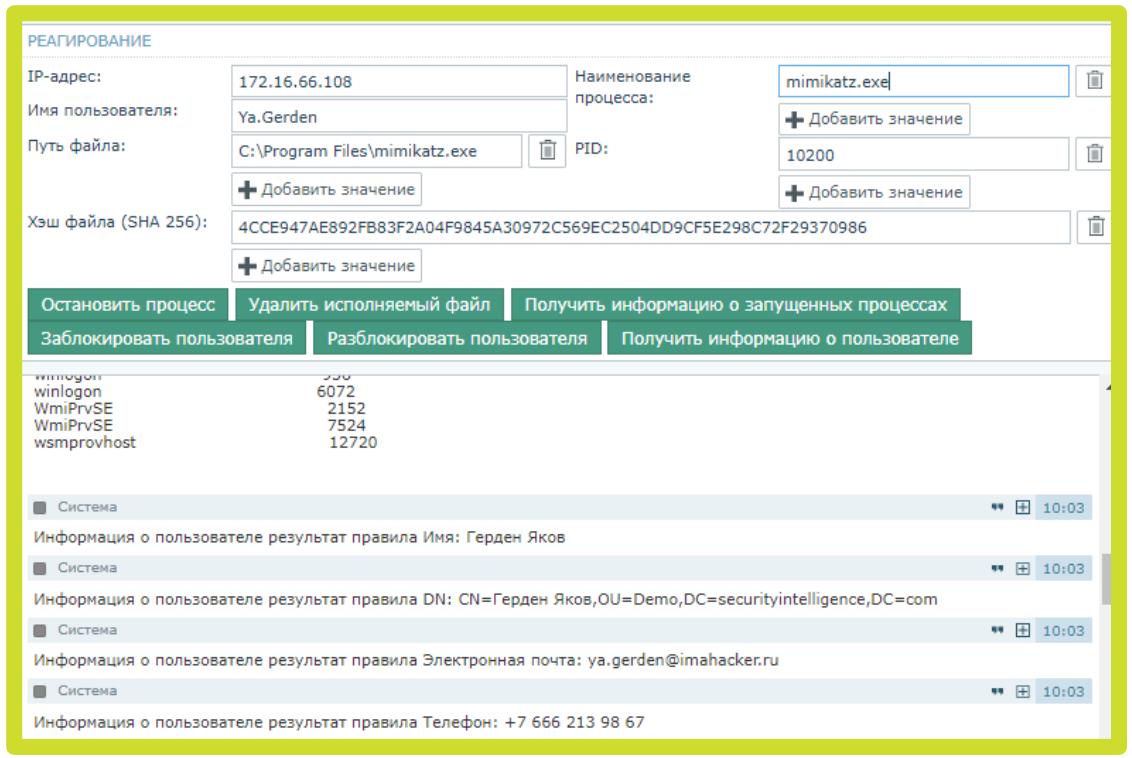
Андрей Амирах

aamirakh@securityvision.ru

Ваш выбор?

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Автоматизируй или страдай!



Национальная банковская премия 2019

Открытие

НАЦИОНАЛЬНАЯ БАНКОВСКАЯ ПРЕМИЯ

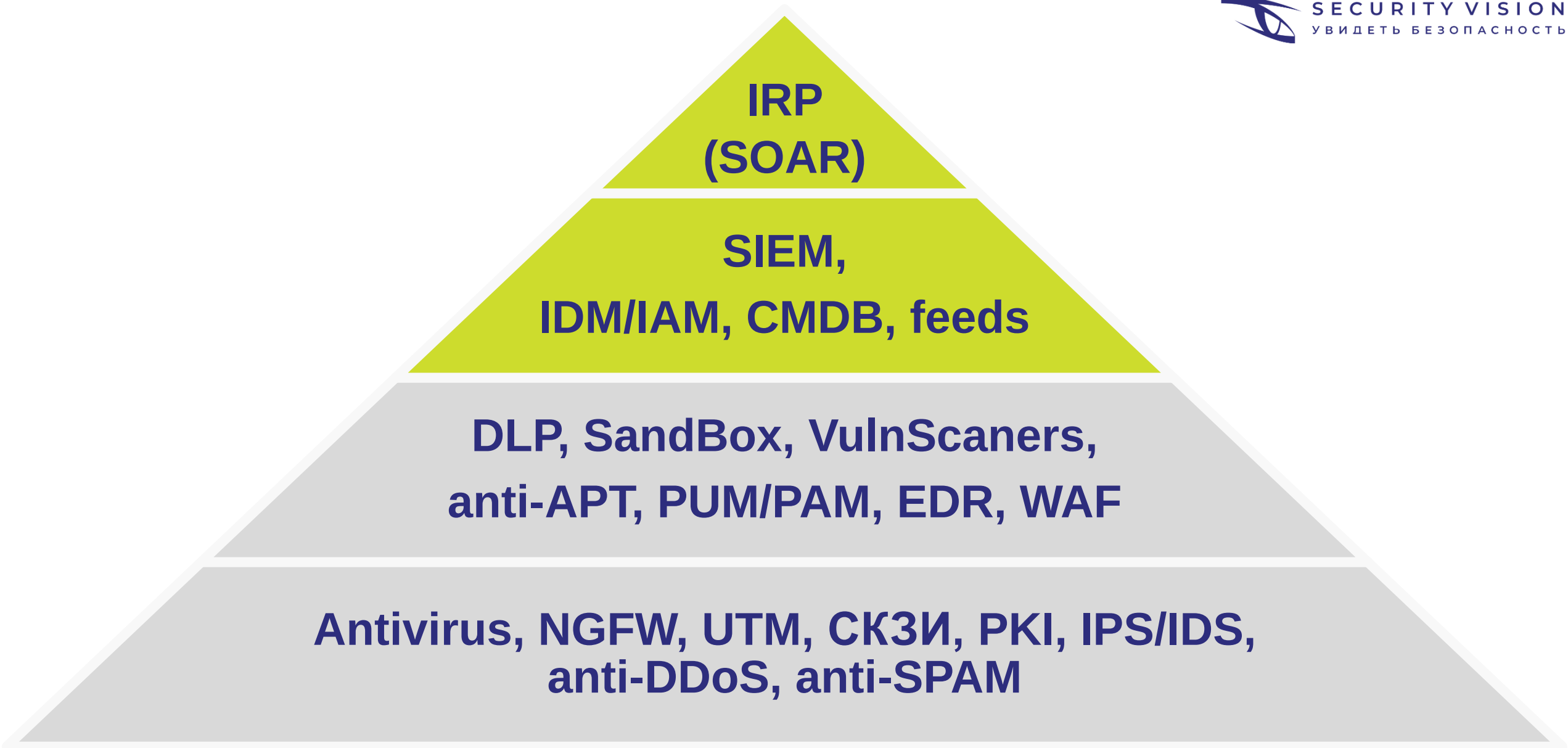
ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ ГРУППА КОМПАНИЙ

Более 30 сценариев

https://www.securityvision.ru/news/security-vision-i-bank-otkrytie-pobediteli-natsionalnoy-bankovskoy-premii/

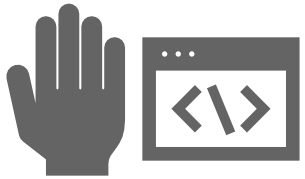
Пирамида уровня зрелости ИБ организаций

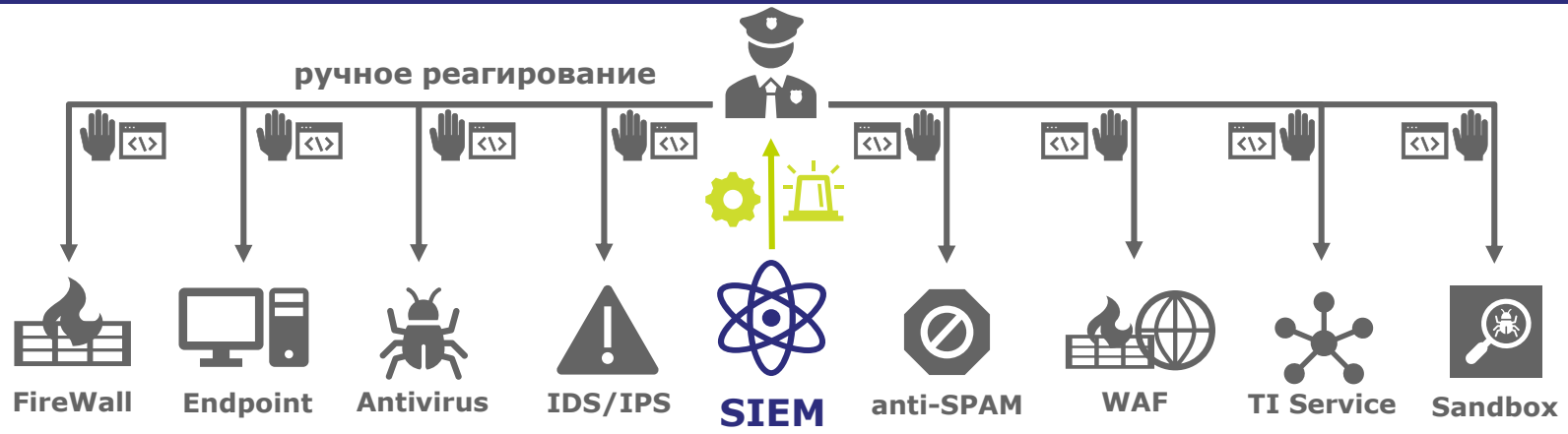
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ



«ДО» И «ПОСЛЕ» внедрения IRP (SOAR)

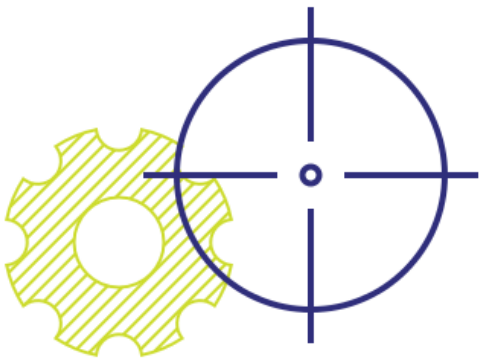
ДО

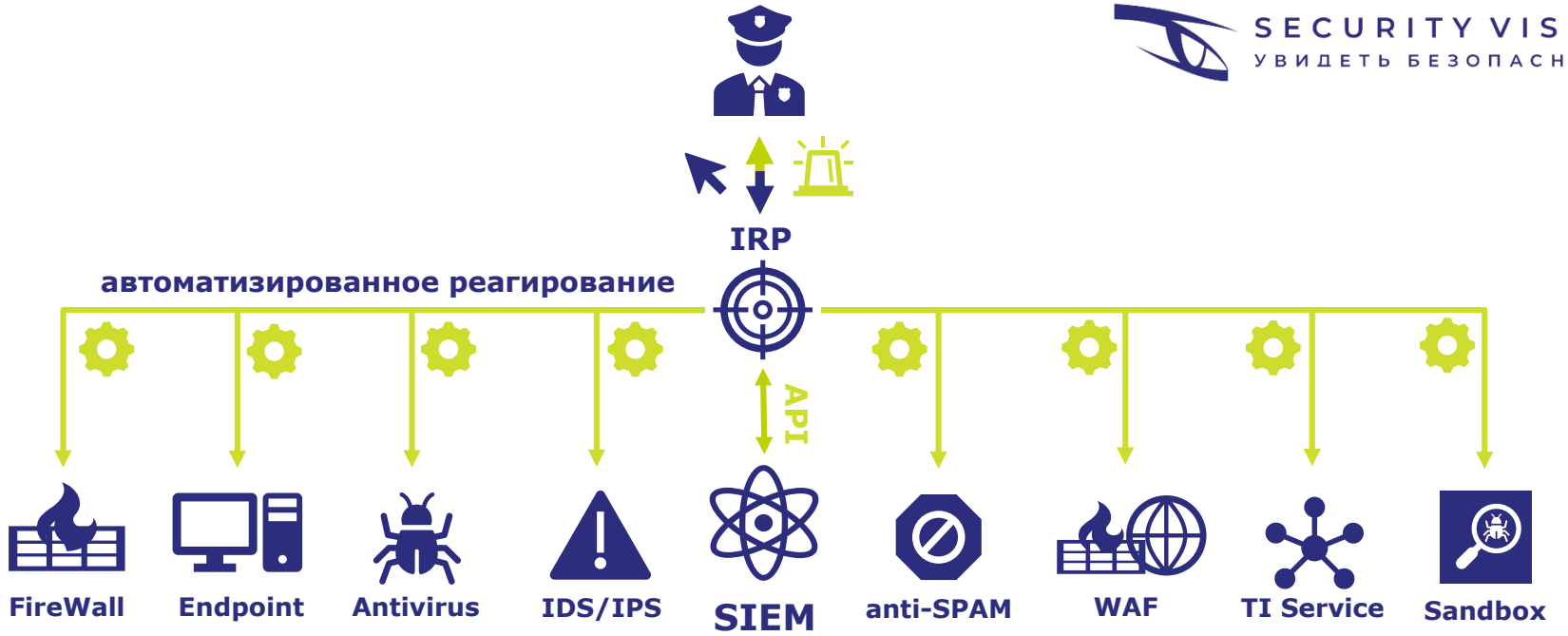




ПОСЛЕ

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

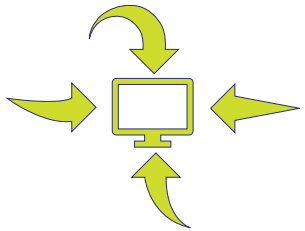




Основные типы сценариев реагирования в IRP (SOAR)

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

1



Обогащение и расследование

2

Предотвращение и устранение

3

Уязвимости (патчинг) и взаимодействие с регуляторами

1.Обогащение и расследование в IRP (SOAR)

1.1 Получение и анализ хеш-суммы, IP, URL и домена на интернет сервисах

1.2 Сбор информации о текущих сессиях по подозрительному IP-адресу от МСЭ

1.3 Отправка подозрительного файла на анализ в песочницу и получение результата

1.4 Получение актуальной информации об учетной записи: ФИО, телефон, почта, должность…

1.5 Получение информации по запущенным процессам на конечном устройстве

1.6 Получение дополнительной информации из SIEM-систем (поиск индикаторов на других хостах)

2. Предотвращение и устранение в IRP (SOAR)

2.1 Блокировка IP, URL, домена на МСЭ / Шлюзе-Email Security Gateway

2.2 Удаление подозрительного файла на конечном устройстве / из почты

2.3 Изоляция/отключение подозрительных хостов

2.4 Инициализация оператором блокировки учетной записи или сброс пароля

2.5 Остановка запущенного подозрительного процесса на конечном устройстве

2.6 Инициализация оператором полного сканирования конечного устройства

3. Уязвимости (патчинг) и регуляторы в IRP (SOAR)

3.1 Автоматический запуск сканирования подозрительного хоста

MaxPatrol 8

Nessus® vulnerability scanner

3.2 Автоматическое создание тикета в ITSM и отслеживание статуса исполнения

Service Manager hp

OTRS

3.3 Автоматическая отправка информации об инцидентах

БАНК РОССИИ ФИНЦЕРТ

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

3.4 Автоматическое обогащение СЗИ индикаторами от регуляторов и сервисов

БАНК РОССИИ ФИНЦЕРТ

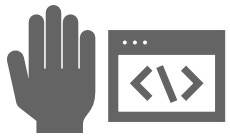
НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

GROUP IB

Оценка эффекта автоматизации реагирования

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

1

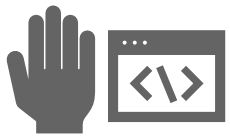


5-45 минут

Обогащение и расследование

~ до 10 секунд
на один сценарий

2

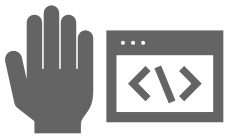


20-300 минут

Предотвращение и устранение

~ до 15 секунд
на один сценарий

3



5-30 минут

Уязвимости (патчинг) и взаимодействие с регуляторами

~ до 10 секунд
на один сценарий

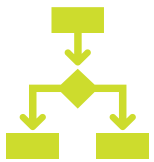
Итоговый профит от IRP (SOAR)

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Сокращение времени реакции на инциденты => снижение ущерба

Высвобождение человеческих ресурсов => экономим ФОТ

Исключение человеческого фактора => снижаем риски (+нет лишних доступов)



Формализация всех процессов, контроль и статистика => повышаем эффективность

Контакты

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Спасибо за внимание!

Андрей Амирах

aamirakh@securityvision.ru

8(495) 803-3660 (доб.108)

ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ ГРУППА КОМПАНИЙ

С нами **работают**

СБЕРБАНК · Ростех · Открытие · ГОЗНАК · ПФР · ГАЗПРОМ-МЕДИА · ФСО РОССИИ

МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ · ГЛАВГОСЭКСПЕРТИЗА РОССИИ · РЧС · СДМ-БАНК · Мультикарта · ГМСгруппа · Корпорация МСП