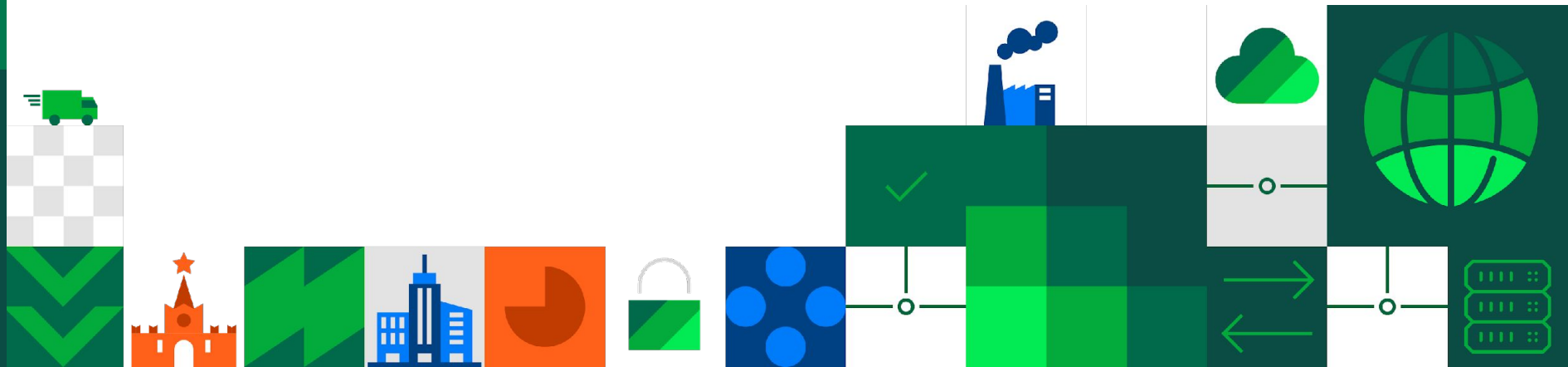
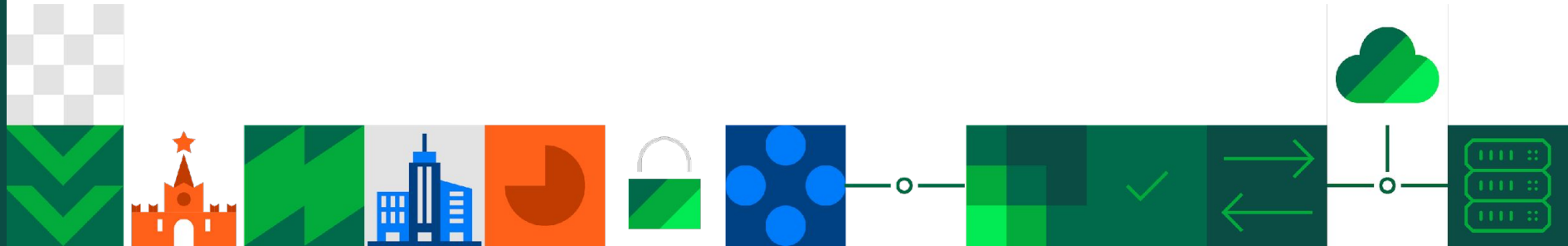
КОД безопасности

Континент WAF 2



КОД безопасности

О продукте



КОД безопасности

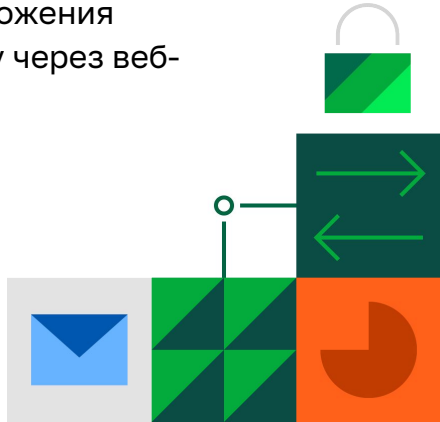
О продукте

Континент WAF 2

Система защиты веб-приложений с автоматизированным анализом бизнес-логики

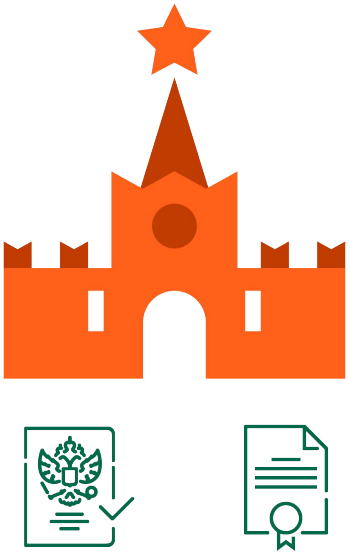
Предназначен для решения следующих задач:

- Защита от кражи данных веб-приложений
- Защита от отказа в обслуживании или замедления работы сервера, обслуживающего веб-приложения
- Защита от проникновения в инфраструктуру через веб-приложения
- Защита от deface атак
- Выполнение требований регуляторов



КОД безопасности

Планы по сертификации



ФСТЭК России

- 4-й класс защиты МЭ типа «Г»

Будет сертифицирован для защиты

- ГИС до до 1 класса защищенности включительно
- ИСПДн до класса УЗ1 включительно
- АС до класса 1Г включительно

КОД безопасности

Возможности продукта

Анализ трафика

- Гибкая настройка моделей работы приложений
- Автоматическое построение модели работы приложения (профилирование)
- Анализ отклонений поведений пользователя от стандартного сценария
- Анализ данных в SSL-туннеле
- Пакет преднастроенных сигнатур
- Поддержка правил формата ModSecurity
- Расширение доступных для разбора структур передаваемых данных
- Возможность выбора различных объектов в качестве источника анализа данных (IP-адрес, сессионный идентификатор и т.д.)
- Проверка успешности действий пользователя и контроль последовательности действий (уровень бизнес-логики)

КОД безопасности

Возможности продукта

Управление и мониторинг

- Графическое отображение модели разбора запросов и ответов веб-сервера
- Мониторинг и управление защитой нескольких приложений из единой консоли
- Графическое отображение и редактирование правил принятия решений
- Вывод обобщенной статистики в режиме реального времени
- Агрегирование и приоритизация данных и Автоматическое оповещение оператора о событиях ИБ
- Ролевая модель доступа в консоль управления
- Аудит действий оператора WAF в консоли управления
- Интеграция с SIEM-системами по протоколу syslog
- Обновление правил ModSecurity в соответствии с OWASP Top 10
- Возможность создания списков объектов для дальнейшего использования в правилах

КОД безопасности

Возможности продукта

Обнаружение атак на веб-приложения

- Обнаружение специфических для веб-приложений атак
  - OWASP TOP 10
  - Bruteforce-атаки
  - DoS на уровне приложений
  - Атаки на механизмы авторизации и аутентификации
- Обнаружение аномалий в запросах и в ответах веб-сервера
- Обнаружение аномалий на основе модели работы приложения
  - Совпадение с моделью
  - Отклонение от модели
- Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP

КОД безопасности

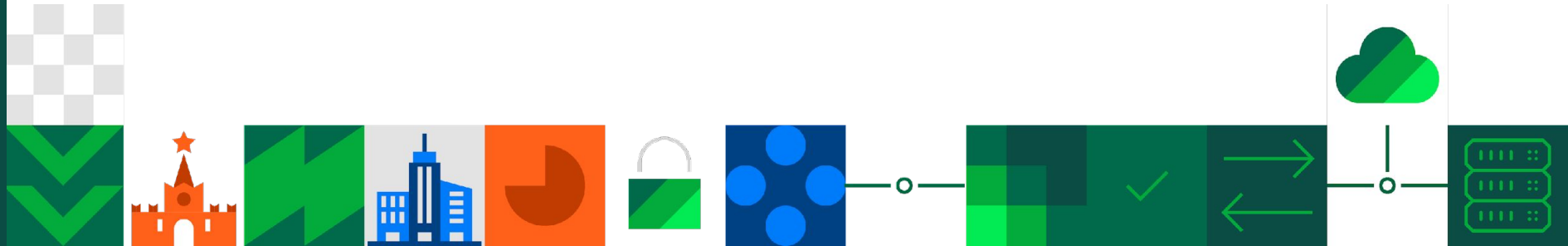
Возможности продукта

Режим работы

- Работа в режиме мониторинга
- Работа "в разрыв" (Reverse Proxy)
- Работа в режиме аудита
  - Анализ логов активности веб-сервера

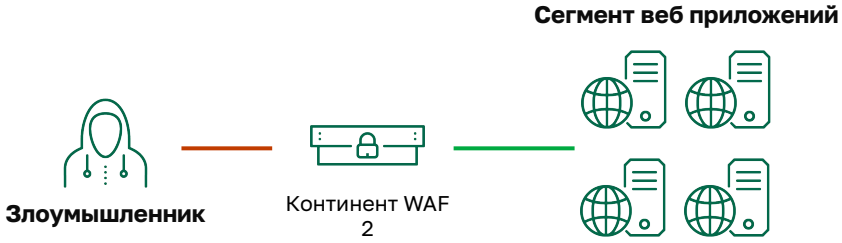
КОД безопасности

Варианты применения



КОД безопасности

Защита веб-приложения



Задачи

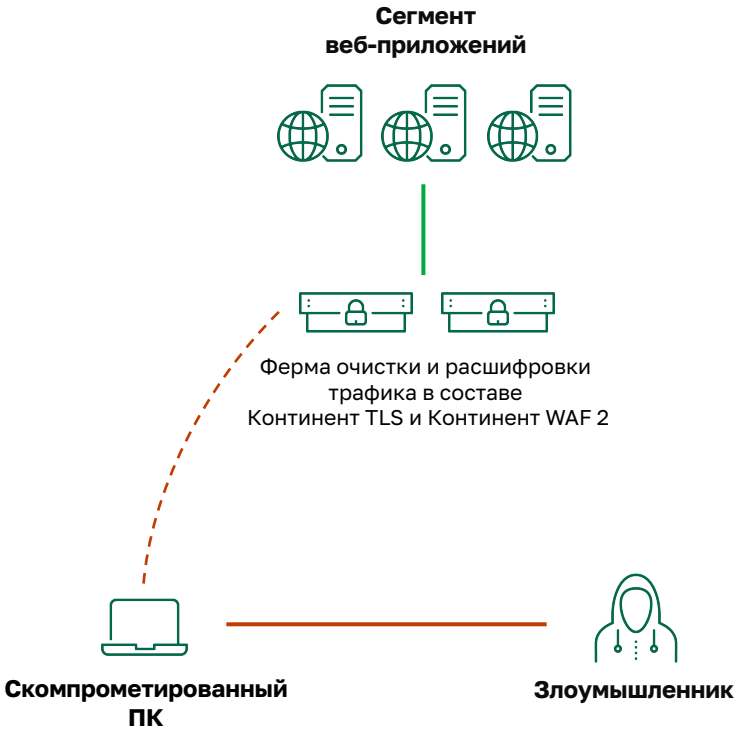
- Защита публичных веб-приложений
- Защита личного кабинета пользователя
- Защита систем межведомственного взаимодействия
- Защита мобильных приложений
- Защита веб-интерфейсов критичных систем

Компоненты

- Континент WAF 2

КОД безопасности

Защита веб-приложения



Задачи

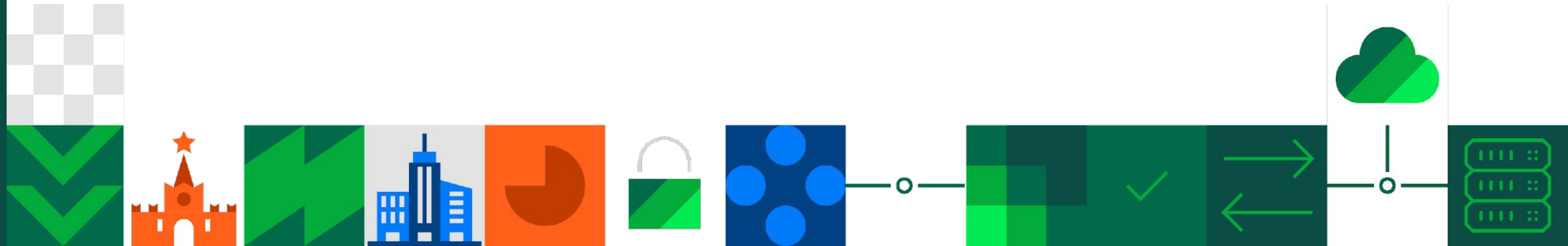
- Защита систем дистанционного банковского обслуживания для юридических лиц
- Защита порталов государственных ведомств

Компоненты

- Континент WAF 2

КОД безопасности

Компоненты



КОД безопасности

Мониторинг и аудит событий

Континент WAF 2

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

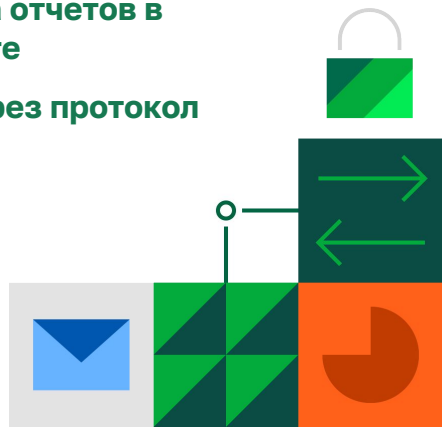
Вывод обобщенной статистики в режиме реального времени

Агрегирование и приоритезация данных о событиях ИБ

Автоматическое оповещение оператора Континент WAF по электронной почте

Генерация и регулярная рассылка отчетов в формате PDF по электронной почте

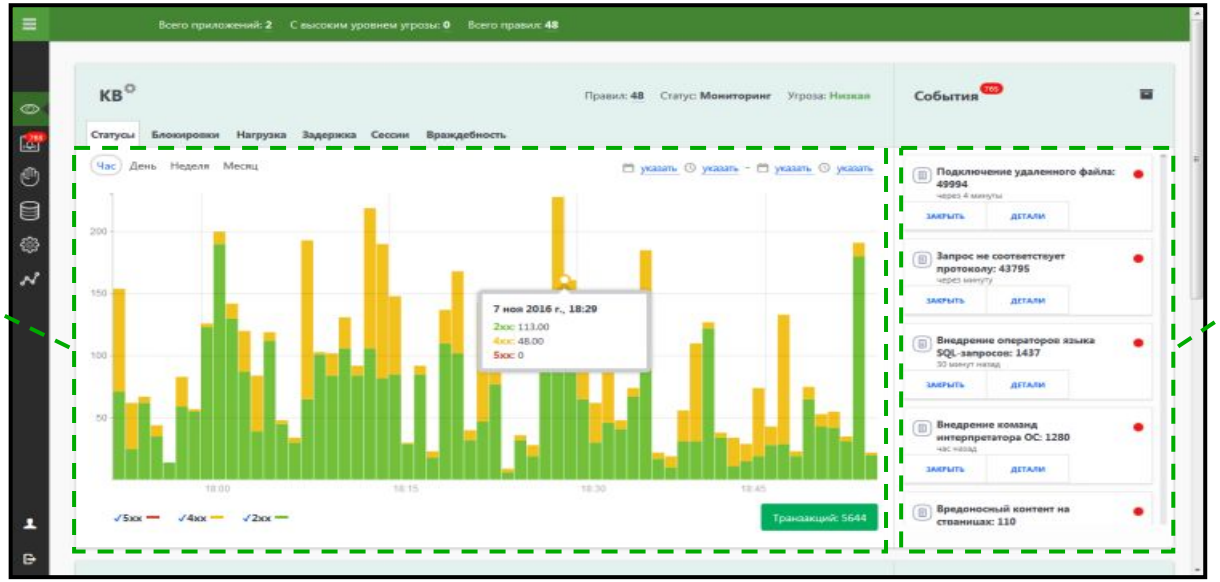
Интеграция с SIEM-системами через протокол syslog



КОД безопасности

Состояние веб-приложений

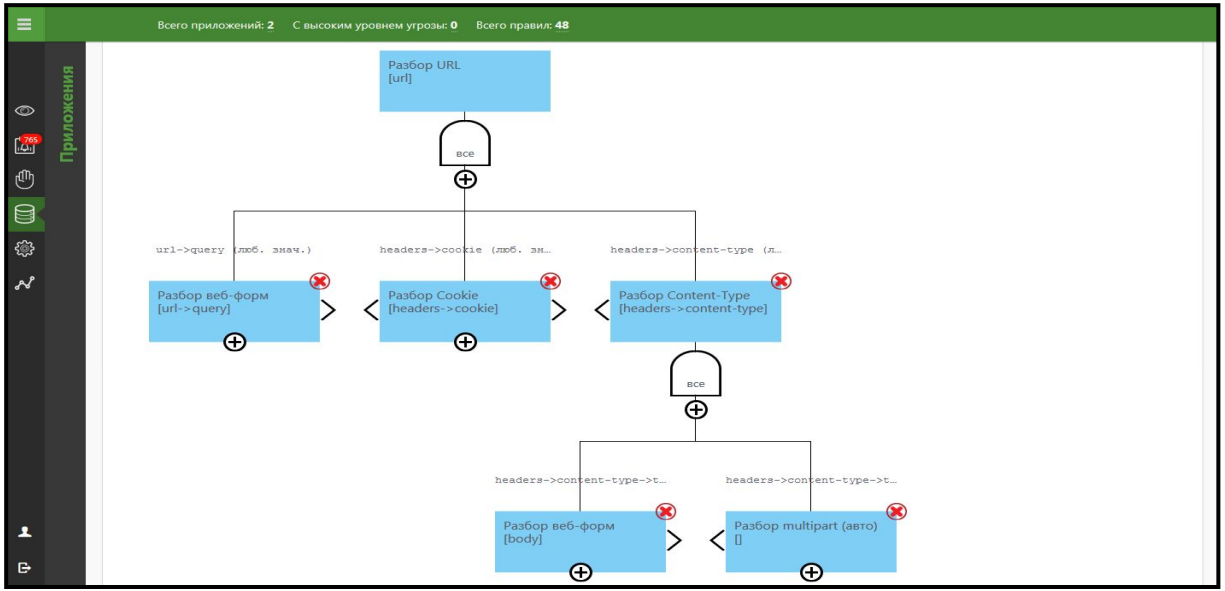
Статистика HTTP-ответов



Последние сработавшие правила

КОД безопасности

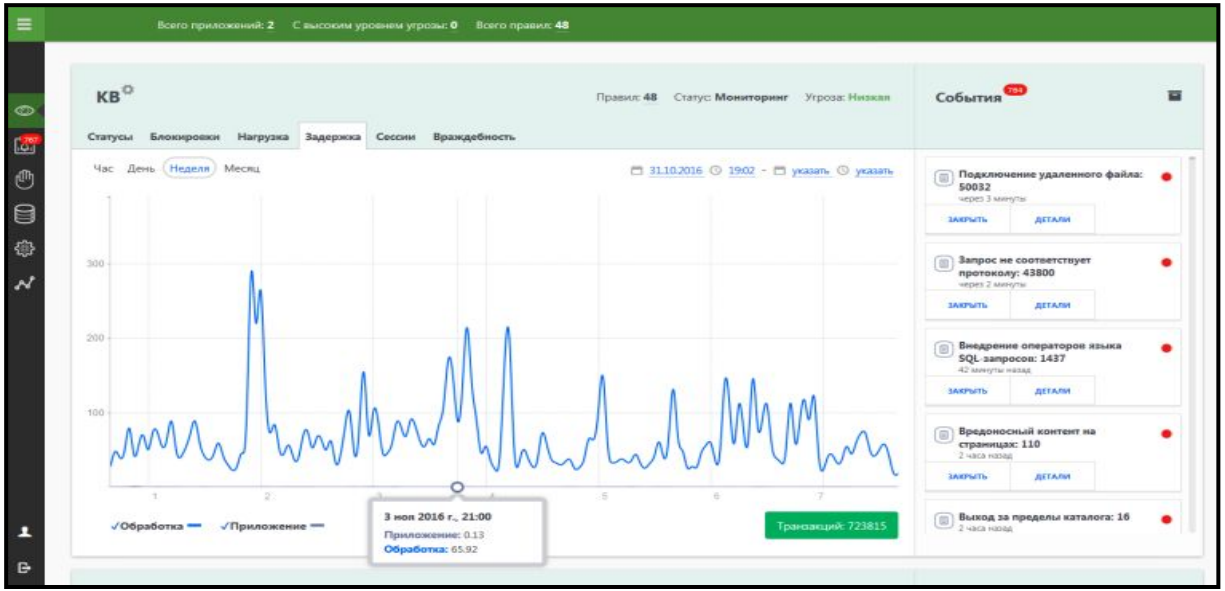
Графическое отображение всех возможных HTTP-запросов и ответов



Дерево разбора HTTP-запросов и ответов веб-приложения для построения модели работы и правил принятия решений

КОД безопасности

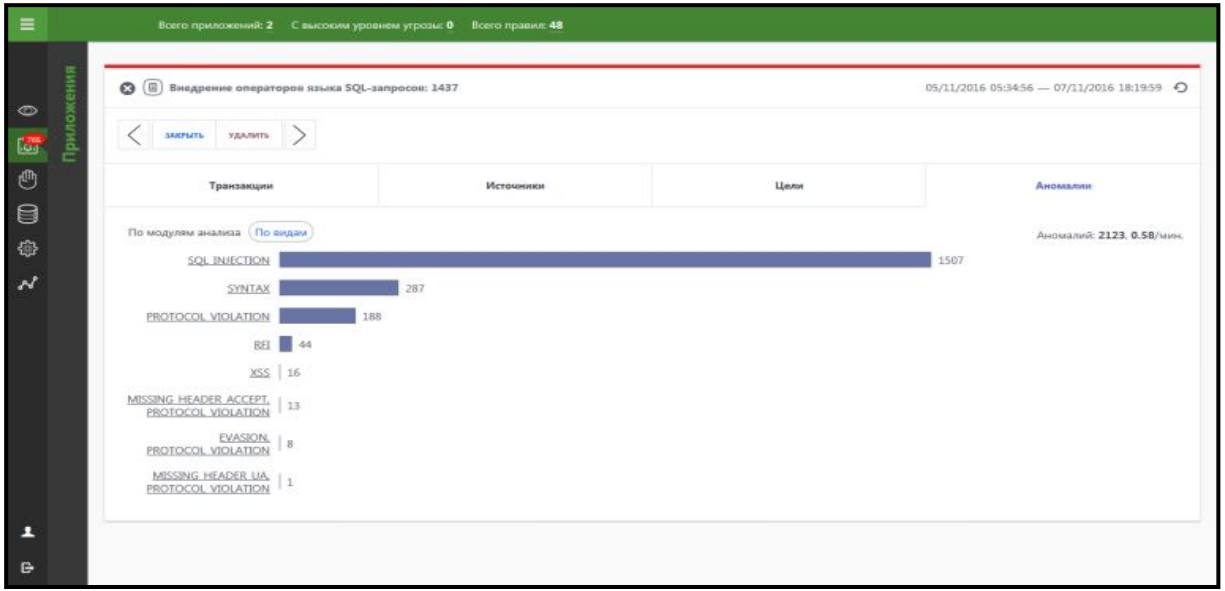
Информация об аномалиях



Статистика задержек ответов веб-сервера

КОД безопасности

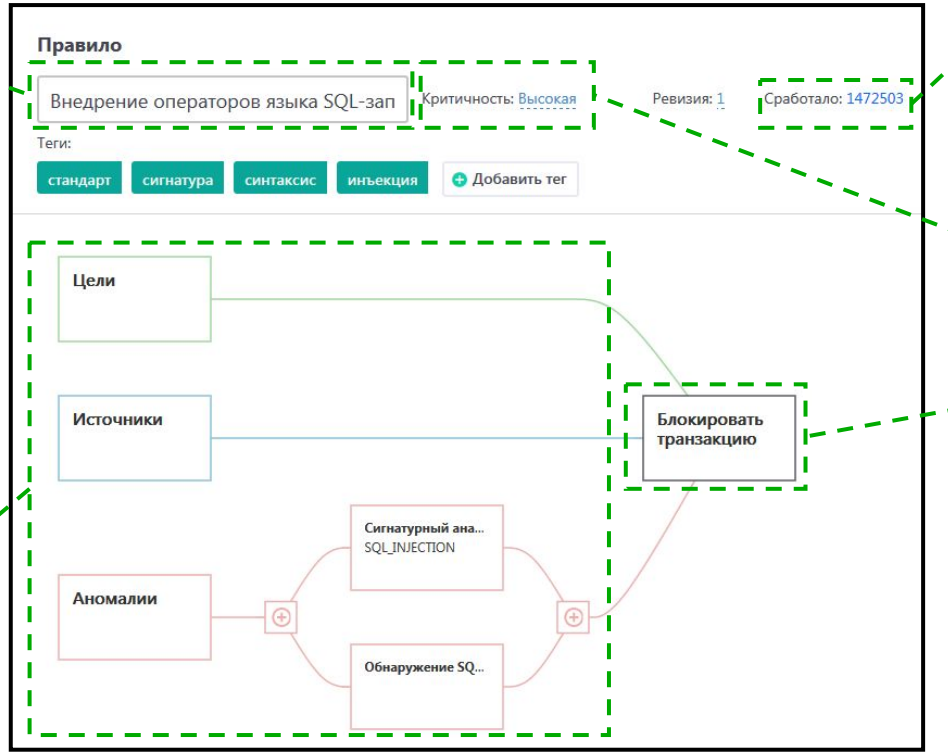
Информация об аномалиях



Распределение по видам аномалий для сработавшего правила

КОД безопасности

Удобный интерфейс редактирования правил принятия решений



Название правила

Число срабатываний правила

Критичность правила

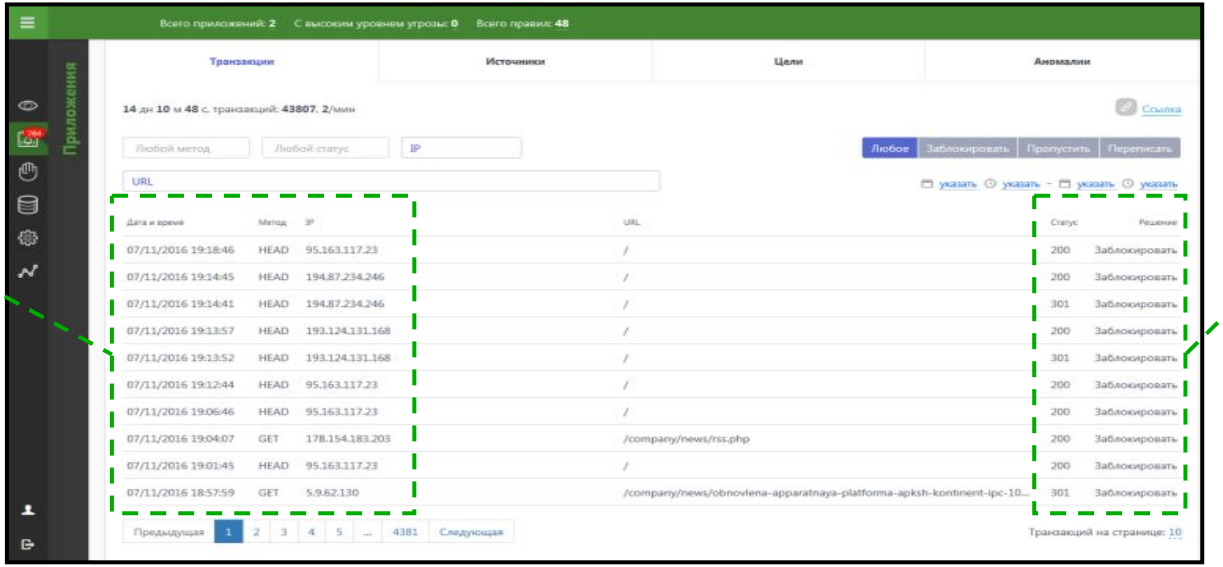
Решение

Условия активации правила

КОД безопасности

Статистика срабатывания правила

Дата и время события, метод, IP-адрес источника атаки



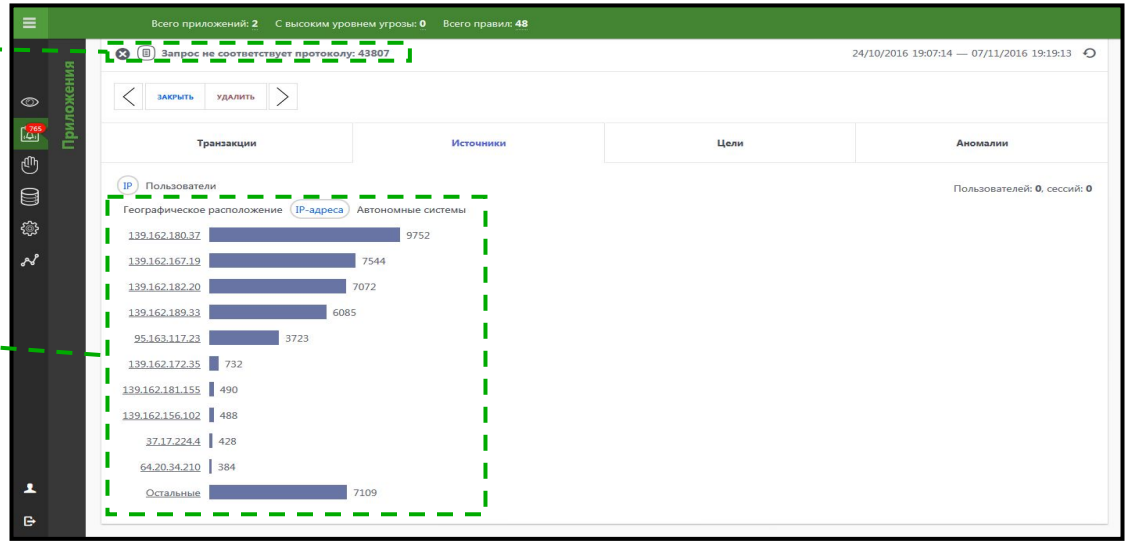
Реакция веб-сервера на запрос и решение о блокировке

КОД безопасности

Статистика источников атак по правилу

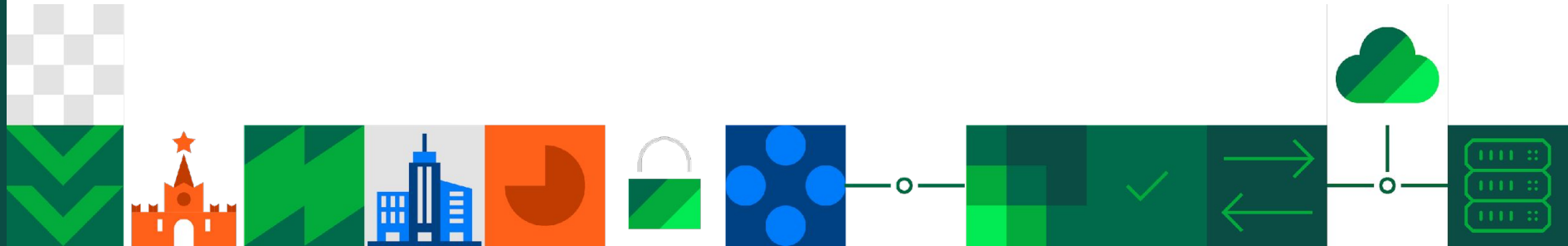
Название правила и число срабатываний

Список источников атак



КОД безопасности

Режимы работы

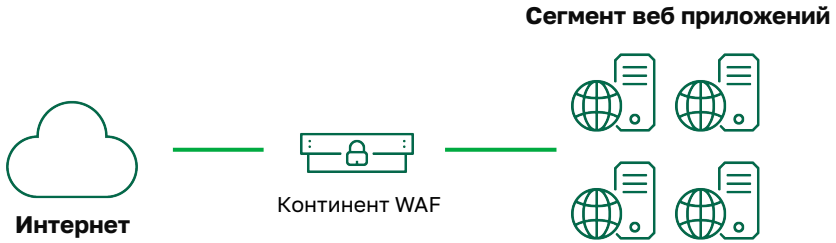


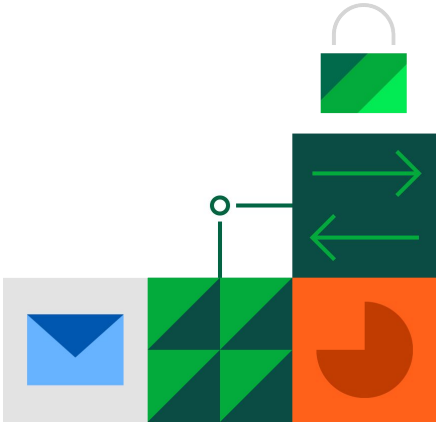
КОД безопасности

Континент WAF в режиме inline

Континент WAF

Блокировка атак
и несанкционированной активности



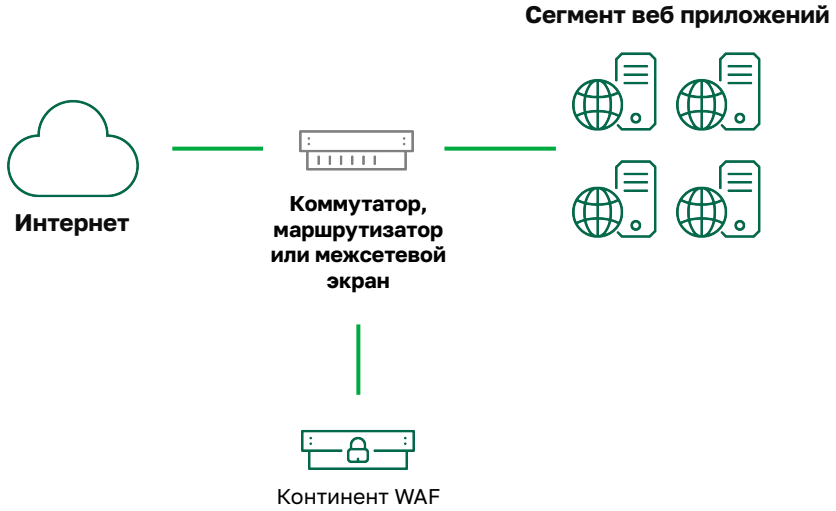


КОД безопасности

Континент WAF в режиме мониторинга

Континент WAF

Обнаружение атак
с информированием оператора

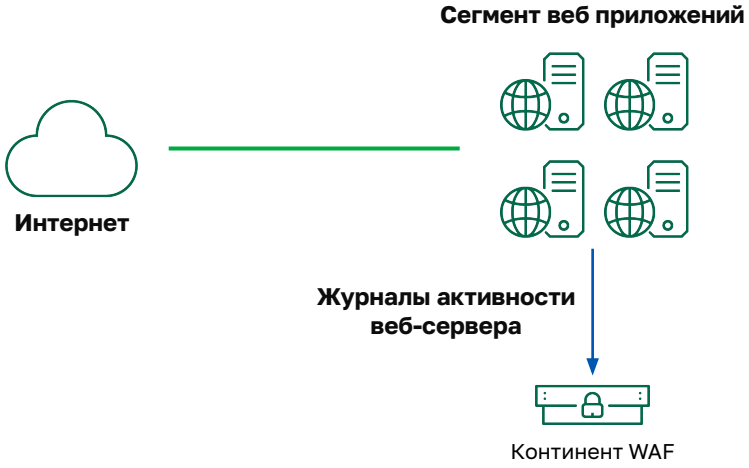


КОД безопасности

Континент WAF в режиме аудита

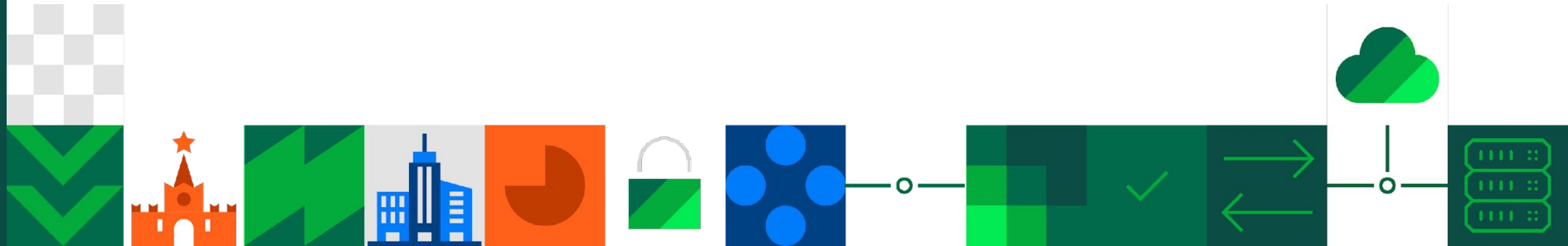
Континент WAF

Обнаружение атак
с информированием оператора



КОД безопасности

Модельный ряд



Континент WAF IPC-R1000

Производительность

- до 1 000 HTTP-запросов в секунду

Сетевые интерфейсы:

- 8 x 10/100/1000BASE-T RJ45
- 4 x 10G SFP+

Формфактор:

- 1U

КОД безопасности

Континент WAF IPC-3000L

Производительность

- до 3 000 HTTP-запросов в секунду

Сетевые интерфейсы:

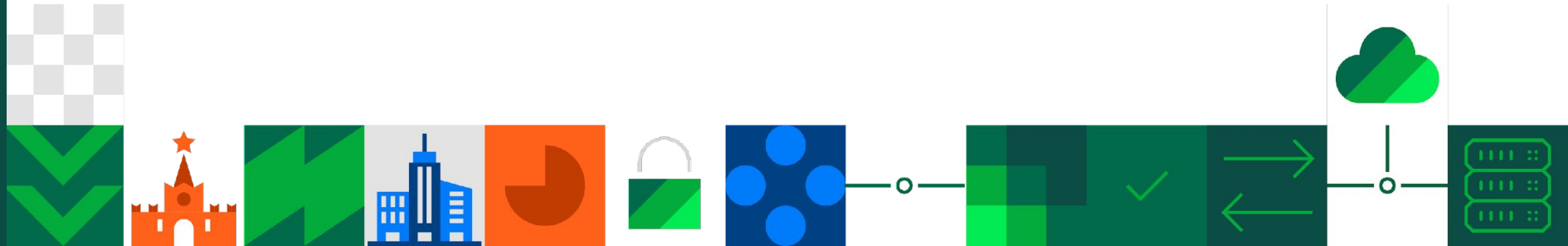
- 1 x 10/100/1000BASE-T RJ45
- 4 x 10G SFP+

Формфактор:

- 1U

КОД безопасности

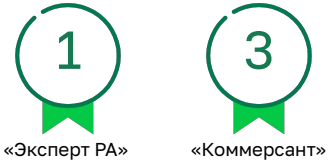
О компании



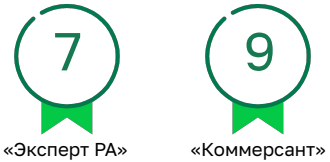
КОД безопасности

Факты о компании

«Крупнейшие производители высокотехнологичного оборудования»



«Крупнейшие разработчики ПО»

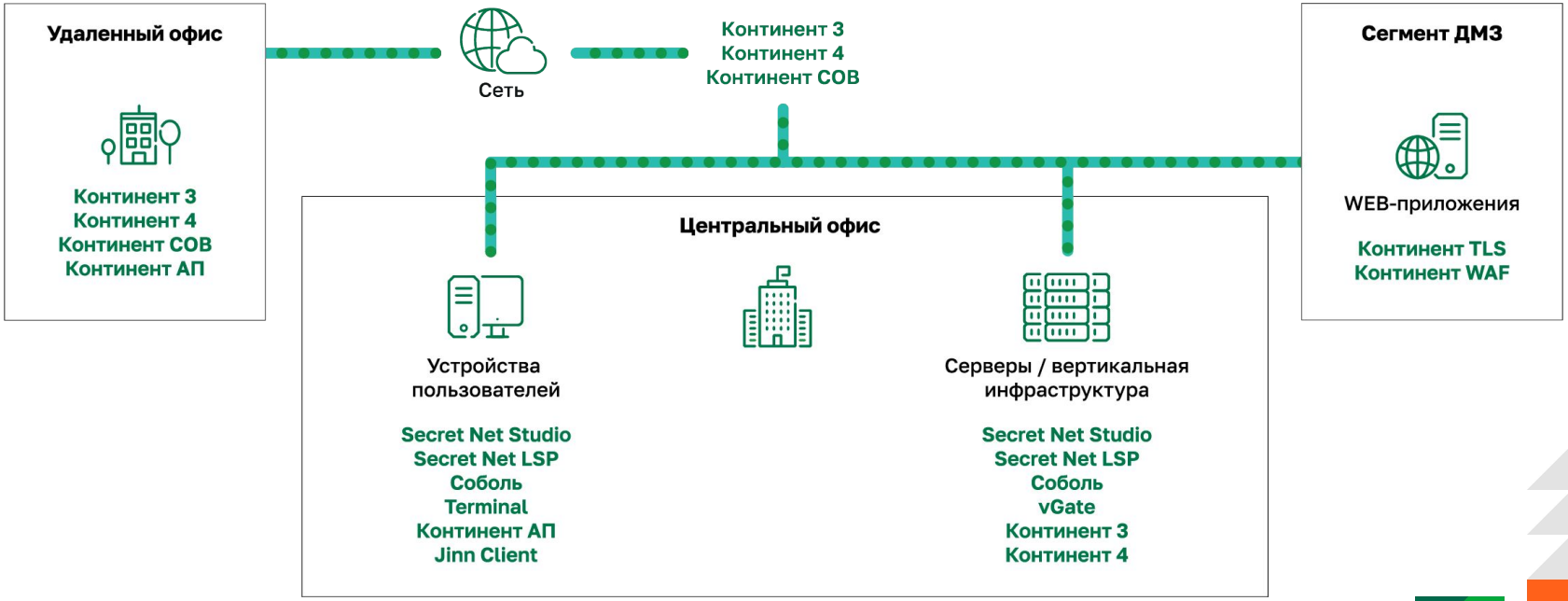


«Крупнейшие ИТ-компании России»

- Более **30 лет** на страже безопасности крупнейших предприятий России
- **9 лицензий** ФСТЭК, ФСБ и Минобороны России
- **3 центра разработки:** Москва, Санкт-Петербург, Пенза
- Более **900 квалифицированных специалистов**, имеющих уникальные компетенции
- Более **50 разработанных СЗИ и СКЗИ**
- Более **60 сертификатов** соответствия
- Обеспечена безопасность **3 000 000 компьютеров** в **50 000 организаций**
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров**

КОД безопасности

Комплексный подход к защите инфраструктуры



КОД безопасности

Нам доверяют

Государственные организации:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный Фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

Силовые структуры:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

Телекоммуникационные компании:

- ПАО «Ростелеком»
- ПАО «МГТС»
- ГК «АКАДО Телеком»
- АО «Военателеком»

Финансовые организации:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- ПАО «Промсвязьбанк»
- Банк ВТБ (ПАО)
- ПАО «Московский кредитный банк»
- АО «АЛЬФА-БАНК»

Промышленные предприятия:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»

Предприятия ТЭК:

- ГК «Росатом»
- ПАО «Газпром»
- ПАО «АК «Транснефть»
- ПАО «НК «Роснефть»»
- ПАО «Россети»

КОД безопасности

info@securitycode.ru
www.securitycode.ru