Информационная безопасность: инструменты и решения

МегаФон

Григорий Айкашев

Менеджер по технологической поддержке облачных и инфраструктурных решений

(Центр, Урал, Сибирь и Дальний Восток)

МегаФон

Атаки 2021 года в России

Атака MoneyTaker на банк, **ущерб 500 млн долларов**

Мошенничество с 3-D Secure, **хищение 400 млн рублей**

Атака на Wildberries, **ущерб 385 млн рублей**

Утечка базы автомобилистов Москвы и Подмосковья, **50 млн наборов ПДн**

Утечка из Hyundai, **1,3 млн наборов ПДн**

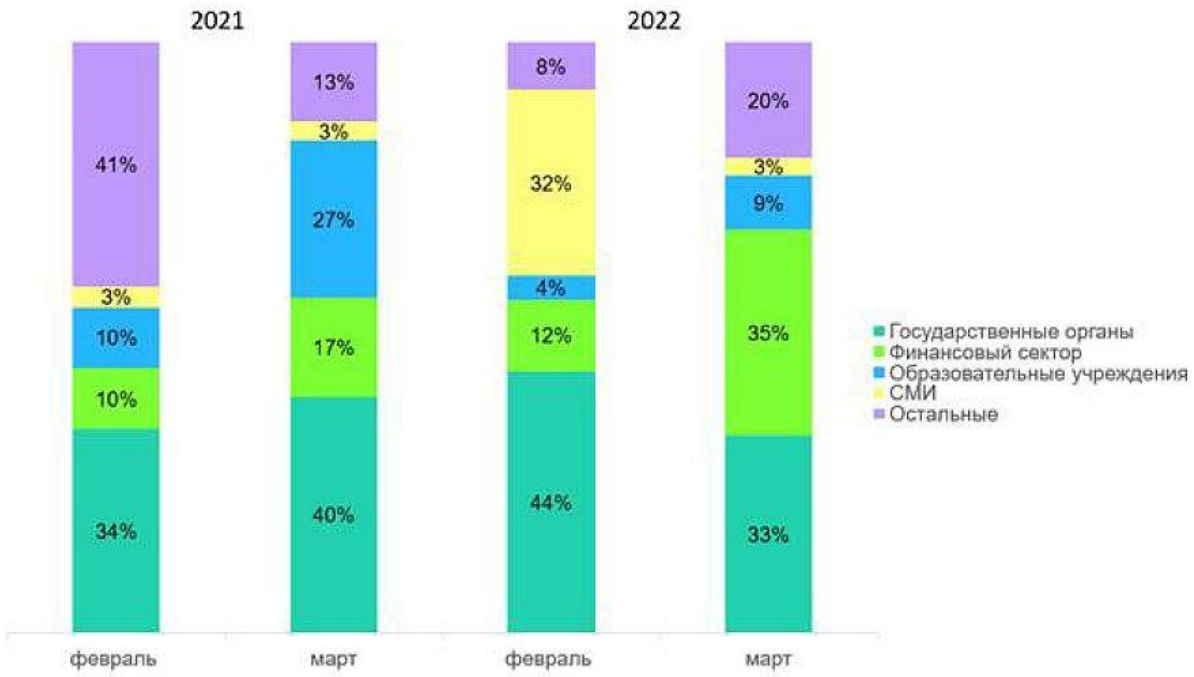
Компрометация ящиков «Яндекса», **утечка данных 5 тыс. ящиков**

…РЖД, Госуслуги, ДОМ.РФ и др.

МегаФон

Источник: https://www.anti-malware.ru/

Kaspersky: в марте число DDoS-атак в России возросло в полтора раза



Специалисты «Лаборатории Касперского» продолжают фиксировать рост количества DDoS-атак на российские организации. Так, в марте этот показатель увеличился на 54% по сравнению с данными за предыдущий месяц; наибольшее число срабатываний защитного решения ИБ-компании было зарегистрировано 25 февраля. В сравнении с мартом 2021 года месячная норма DDoS в рунете возросла в восемь раз.

МегаФон

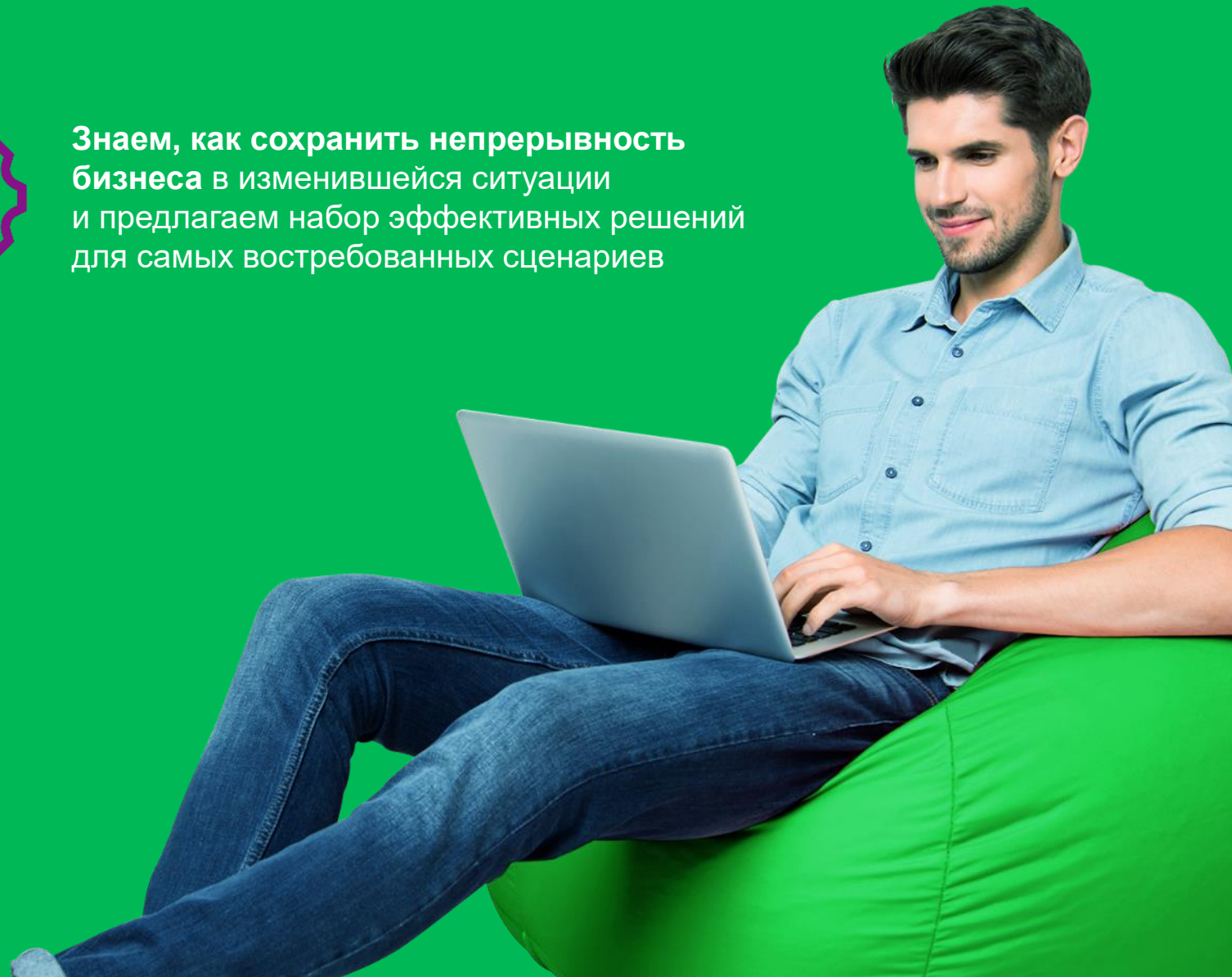
Источник: https://www.anti-malware.ru/,

Опыт и экспертиза МегаФона

Много лет используем собственные продукты для организации удаленной работы

Знаем, как сохранить непрерывность бизнеса в изменившейся ситуации и предлагаем набор эффективных решений для самых востребованных сценариев

Десятки выполненных проектов по кибербезопасности
Собственная экспертиза и опыт по анализу защищенности, внедрению DLP, MDM и т.д.



МегаФон

Экосистема кибербезопасности от МегаФона

Сетевая и web-безопасность

- **Анти-DDoS**
- **WAF**
- **Защита почты**

- DLP
- Защита баз данных
- Криптозащита
- ПАК «Информационный Периметр»

Крупные проекты

- Тестирование защищённости
- Консалтинг и разработка архитектуры систем безопасности
- **Security Awareness**

Экспертные услуги

Защита мобильных устройств

- МегаФон MDM
- Антивзлом Бизнес
- Конфиденциальная сотовая связь

Услуги кибервразведки

- Threat Intelligence
- Голосовой антифрод

МегаФон

Что такое DDoS-атака?

DDoS от англ. Distributed Denial of Services — распределенный отказ в обслуживании

Это сетевая атака, заключающаяся в большом количестве одновременных запросов на сервера компании с целью доведения системы до отказа.

Успешная атака
парализует работу сайта

Пользователи не могут получить к нему доступ, либо он сильно затруднен. Это может привести к серьёзным финансовым и репутационным потерям, вымогательству и т.д.

Защита от атак на уровнях модели OSI

Блокируем масштабные и точечные атаки

Представительский

SSL Exhaustion

Транспортный

Firewall, NAT, DPI UDP Flood, SYN Flood, TCP Flood, TCP State-Exhaustion Attack, NTP Amplification, DNS Amplification, SNMP Amplification, SSDP Amplification, LDAP Amplification, Memcache Amplification,

Канальный

Уровень приложений

SNMP Flood, DNS Flood, SIP Flood HTTP/HTTPS Flood, Slow HTTP, Slow Read и Slowloris

Сеансовый

Сетевой

ICMP Flood

Физический

МегаФон

Услуга «Защита от DDoS-атак»

Решение построено на базе технологий компании «Гарда Технологии» — Российского лидера по разработке систем защиты от DDoS-атак.

Защищает информационные ресурсы от перегрузок и DDoS-атак мощностью до 300 Гбит/с, не прерывая подключения обычных пользователей.

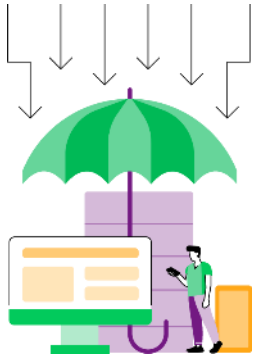
Не замедляет работу ресурса.

Автоматическое отслеживание и очистка трафика. Время включения фильтрации 5-15 сек. благодаря технологии Fast Flood Detection.

Ежедневное обновление базы угроз.

МегаФон

От чего защитит наше решение



Flood Attacks

Атаки, переполняющие каналы связи за счет отправки большого числа запросов, не приводящих к установке соединения и создающих очередь «полуоткрытых соединений». Сервер перестает отвечать, а создание новых подключений невозможно

Amplification Attacks

Атаки с использованием эффекта усиления (амплификатора) для увеличения мощности. Сравнительно небольшие ресурсы злоумышленника становятся причиной значительно большего ущерба или полного отказа работы системы-жертвы

Volumetric Attacks

Атаки, перегружающие каналы или оборудование для препятствования работе сервиса. Уровни OSI 3-4

«Медленные» атаки

Отправка большого числа запросов, передающихся с очень медленной скоростью, из-за чего ресурсы сервера используются гораздо дольше, препятствуя обработке запросов других пользователей

Application Layer Attacks

Атаки на приложения (веб-серверы, серверы баз данных, VoIP-телефонию и т. д.). Уровень OSI 7

МегаФон

Атака на веб-приложение – распространенный инструмент для проникновения в инфраструктуру

19%

В среднем каждая 5-я попытка взлома компании начинается с атаки веб-приложения*

54%

веб-приложений имеют открытую уязвимость**

МегаФон

* Согласно отчету Ростелеком Солар
** Согласно отчету Imperva

Зачем нужен WAF?

Предотвратите утечку данных

Злоумышленники могут взломать сайт и получить доступ к внутренней информации:

- персональные и финансовые данные;
- доступ к ИТ-инфраструктуре.

Предотвращает кражу данных и обеспечит безопасность web-приложений с помощью автоматизированных механизмов защиты.

Усовершенствуйте систему защиты

WAF от МегаФона можно интегрировать в любую систему безопасности незаметно для обычных пользователей:

- отсутствие задержек в работе сайта или приложения;
- интеграции с основными SIEM и DLP-системами;
- интеграция с системами контроля БД;
- сертификация по требованиям ФСТЭК;
- соответствие стандарту PCI DSS (Visa, MasterCard, American Express и JCB).

МегаФон

От чего защитит WAF?

Несанкционированный доступ к данным

Поможет избежать потери данных, раскрытия внутренней информации и кражи конфиденциальных данных. Злоумышленники не смогут скрытно регистрировать, читать, создавать, изменять или удалять записи и права доступа пользователей.

Удаленное срабатывание кода

Злоумышленники не смогут дистанционно запускать выполнение нелегитимных команд, которые провоцируют сканирование внутренних систем компании, деактивацию сайтов или перенаправление пользователей на вредоносные сайты.

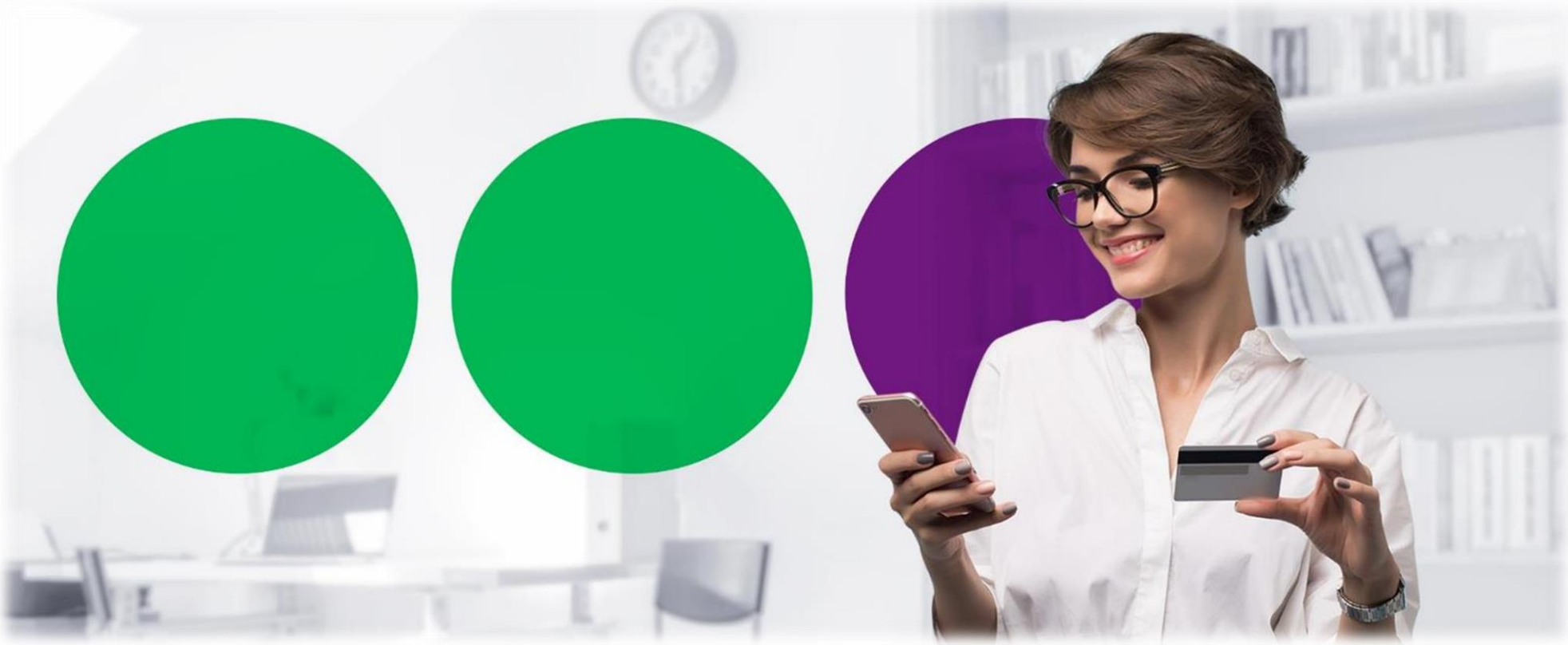
Нарушения в безопасности веб-приложений

Из-за уязвимостей компонентов системы повышается эффективность DoS-атак. Медленное реагирование на атаки позволяет злоумышленникам продолжить извлекать, подделывать и уничтожать данные. WAF поможет выявить и исправить такие нарушения. А так же зарегистрирует потенциальные атаки.

МегаФон

Противостояние социальной инженерии

А именно психологическому манипулированию людьми с целью совершения определенных действий или разглашения конфиденциальной информации.



МегаФон

Вам письмо!

50%

Доля спама
в почтовом трафике

21%

Спама исходило
из России

>184 млн

Вредоносных вложений
обнаружено в письмах
в 2020 году

Чаще всего почтовый антивирус
срабатывал на письма, содержащие
«зловреды» этого семейства

МегаФон

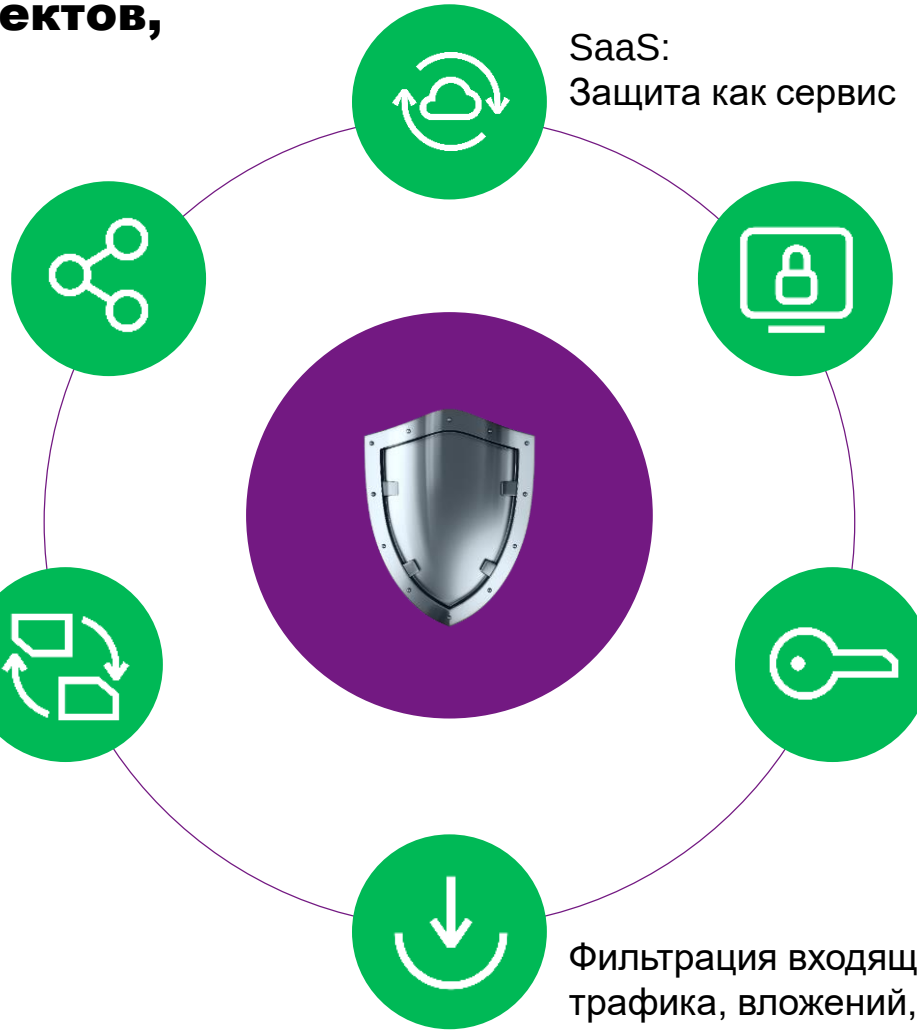
*Исследование Лаборатории Касперского, 2020

Как заставить человека перейти на зараженный ресурс?

МегаФон

Mail Security МегаФон

Сервис для защиты корпоративной почты от вредоносных объектов, спама и фишинга



SaaS:
Защита как сервис

HuMachine™: многоуровневая защита от вредоносного ПО

Проверка подлинности (DKIM, DMARC, SPF)

Фильтрация входящего и исходящего трафика, вложений, анализ фишинга

Нейросетевой анализ

Отказоустойчивость

Возможность интеграций SIEM, SandBox и др..

МегаФон

Полный функционал «Защиты корпоративной почты»

Защита от вредоносных программ

- На основе машинного обучения и облачных вычислений
- В режиме реального времени с повторным сканированием по запросу

Управление безопасностью и отчетность

- Централизованное управление через CLI/GUI
- Контроль доступа на основе ролей
- Подробные отчеты
- Интеграция с SIEM
- Гибкая система регистрации и уведомлений

Гибкое развертывание и интеграция

- Поддерживается несколько платформ и сценариев развертывания
- Интеграция с Microsoft Active Directory
- Интеграция с Kaspersky Anti Targeted Attack Platform

Интеллектуальная защита от спама

- Использует глобально полученные данные из облака
- Раннее предупреждение и блокировка волн спама

Антифишинг

- Глубокое обучение и прикладная лингвистика
- Обнаружение мошеннических действий, не связанных с вредоносным ПО
- Борьба с компрометацией корпоративной электронной почты с помощью специально разработанных алгоритмов

Контроль передачи данных

- Расширенная фильтрация содержимого с распознаванием истинного типа файла и сложным текстовым поиском
- Списки надежных и ненадежных отправителей и получателей

МегаФон

Обучающая платформа Security Awareness —

платформа для повышения осведомленности
сотрудников в сфере информационной безопасности
с понятным запоминающимся контентом
и возможностью проверить знания

МегаФон

Что содержит платформа SA?

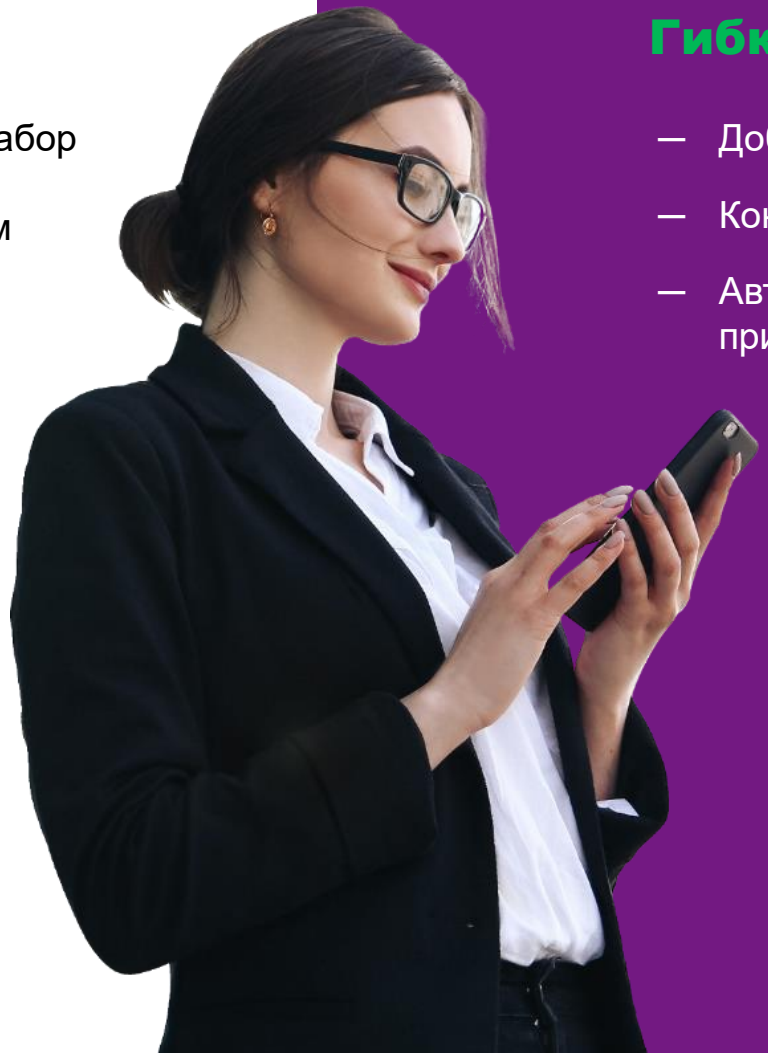
Набор курсов

Платформа содержит в себе материалы и набор теоретических блоков — всё необходимое для обучения базовым понятиям и правилам работы с информационными ресурсами.

Имитация фишинга

Встроенный в систему фишинговый модуль с множеством настроек. Фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

МегаФон



Гибкость и контроль

- Добавление собственных курсов
- Контроль процесса прохождения курсов
- Автоматизация процесса обучения при помощи гибкой системы

Что делать?

Знать векторы атак и защищаться!

МегаФон

МегаФон SOC

Security Operation Center – коммерческий центр мониторинга и реагирования на инциденты ИБ в режиме 24/7

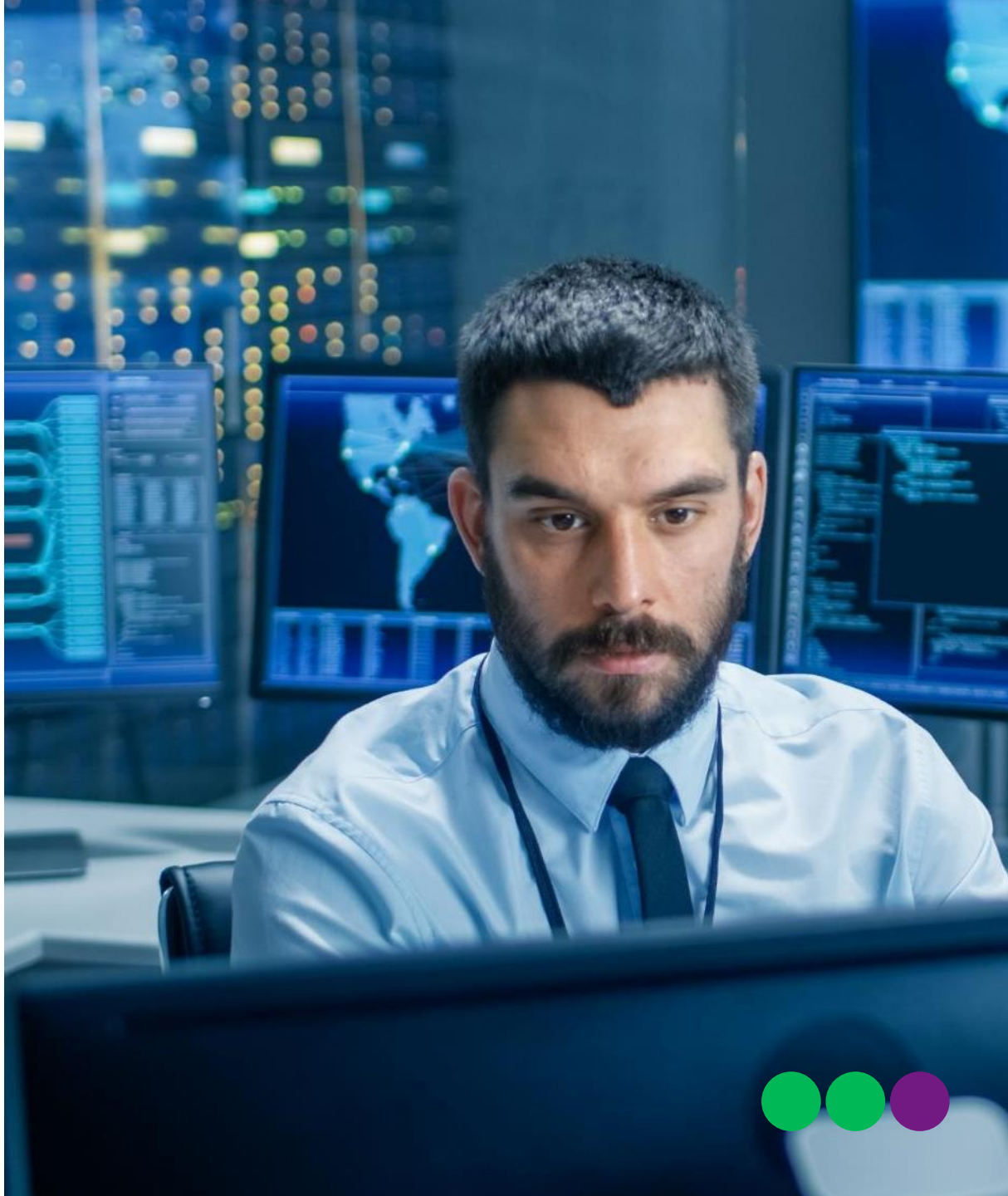
Агрегация событий ИБ
из разных источников

Анализ событий
и инцидентов ИБ

Реагирование
на инциденты

Отчетность и
визуализация данных

МегаФон



Контакты

Григорий Айкашев
Менеджер по технологической поддержке
облачных и инфраструктурных решений
(Центр, Урал, Сибирь и Дальний Восток)

Mobile: **+7 965 99 99 054**
E-mail: Grigory.Aykashev@MegaFon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон