softline®
Мы всё сможем

Трансформация.
Успешная. Цифровая. Защищенная.

Защита инфраструктуры.

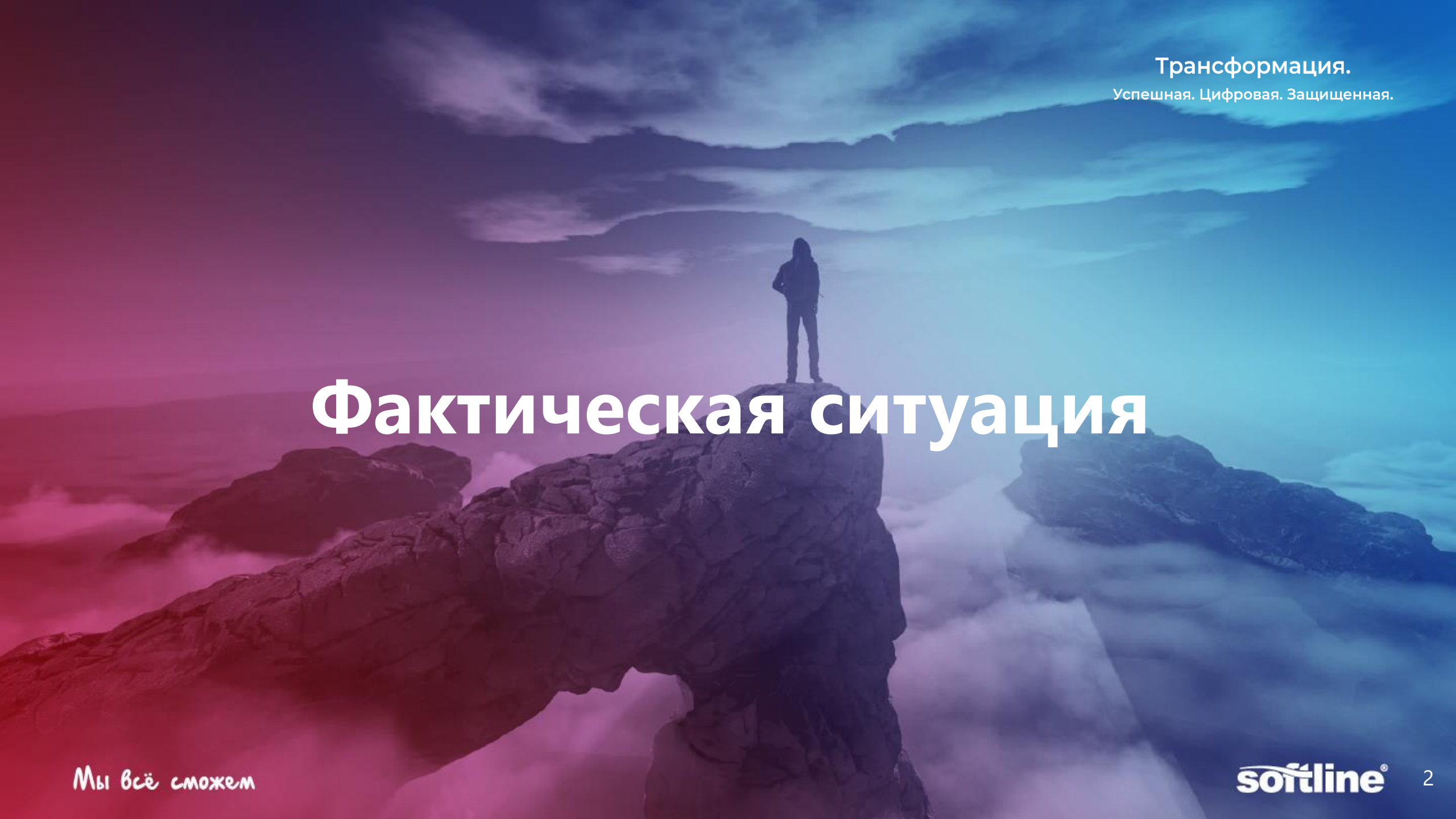
Безопасность сетевого периметра (NGFW) - Usergate

Шкатов Александр

Менеджер группы развития продаж решений информационной безопасности в ЦФО

T +79601171278

Alexander.Shkatov@softline.com



Фактическая ситуация

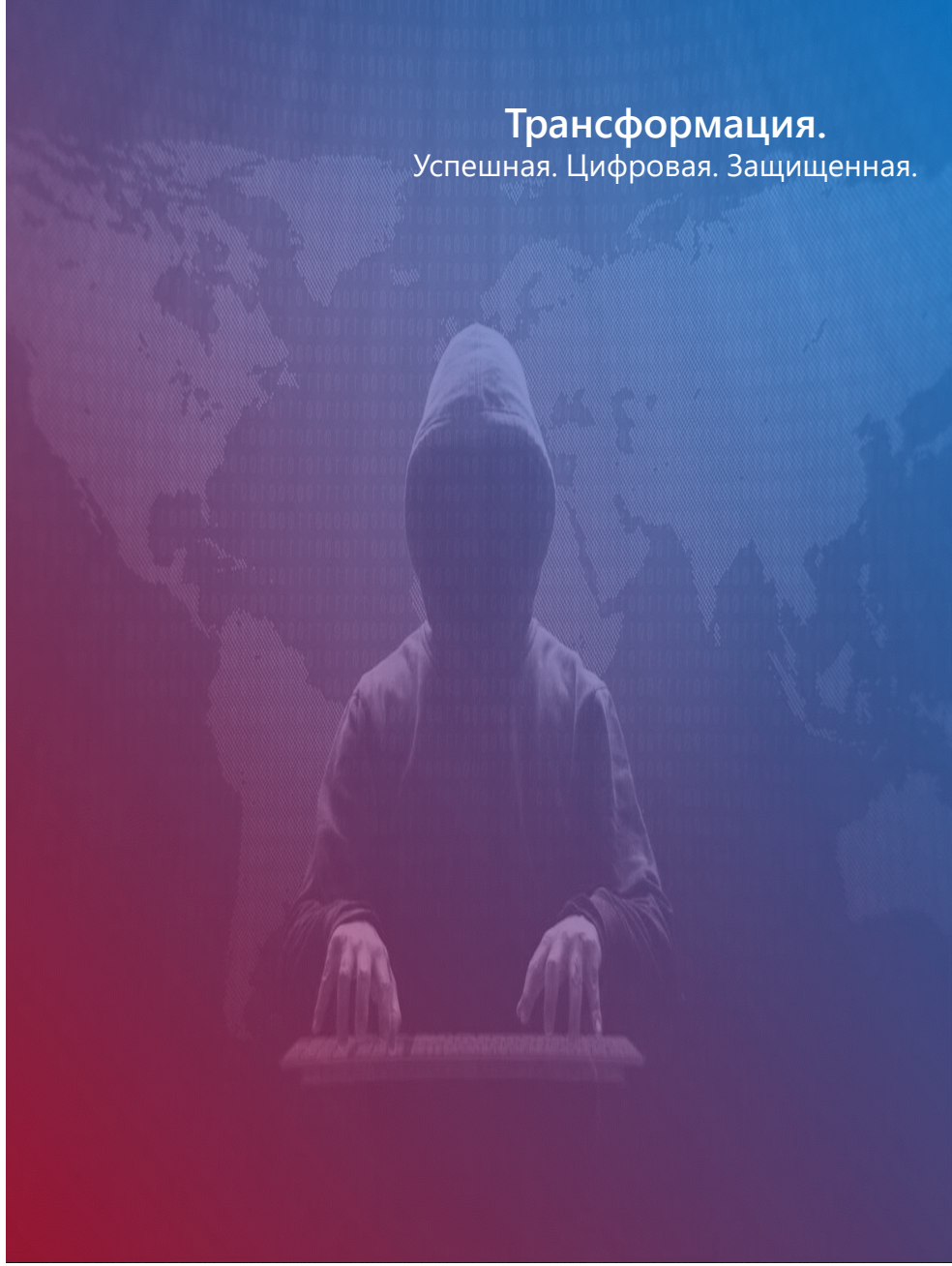
Угрозы кибербезопасности

Статистика на территории Российской Федерации

Кратный рост числа кибер-атак:
- Государственные организации
- Банки
- Сайты СМИ

32%
Доля умных атак

Векторы атак:
RUS, РУС, РОС, .ru, .рф и др.



Ландшафт угроз сетевой безопасности

Черви, вирусы, трояны, backdoors и вымогатели – наиболее распространённые типы вредоносов

Вирусы и черви (Viruses & worms)
(WannaCry, Petya, Xafecopy Trojan, Kedi RAT, Thanatos, Titanium)

Фишинг и соц.инженерия (Phishing)
(email, business email compromise (BEC), company impersonation, websites)

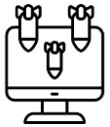
Эксплойты, уязвимости (Exploit Kits)
EK: Spelevo, Fallout, Magnitude, RIG, GrandSoft, Underminer, KaiXin, Purplefox, Capesand)

Теневые загрузки (Drive-by Download)
(LoadPCBanker, YoukuTudou и другие вредоносные сайты)

Отказ в обслуживании (Denial of Service)
(LDAP amplification, DNS-service Router 53, Flood: ICMP, HTTP, TCP, UDP)

Шифровальщики (Ransomware)
(STOP (DJVU), Dharma, Phobos, GlobeImposter, REvil, GandCrab, Magniber, Scarab, Rapid, Troldesh)

Криптомайнинг (Cryptojacking)
(in-browser (websites, cryptomining scripts), Coinhive (JavaScript miner), Cryptoloot)



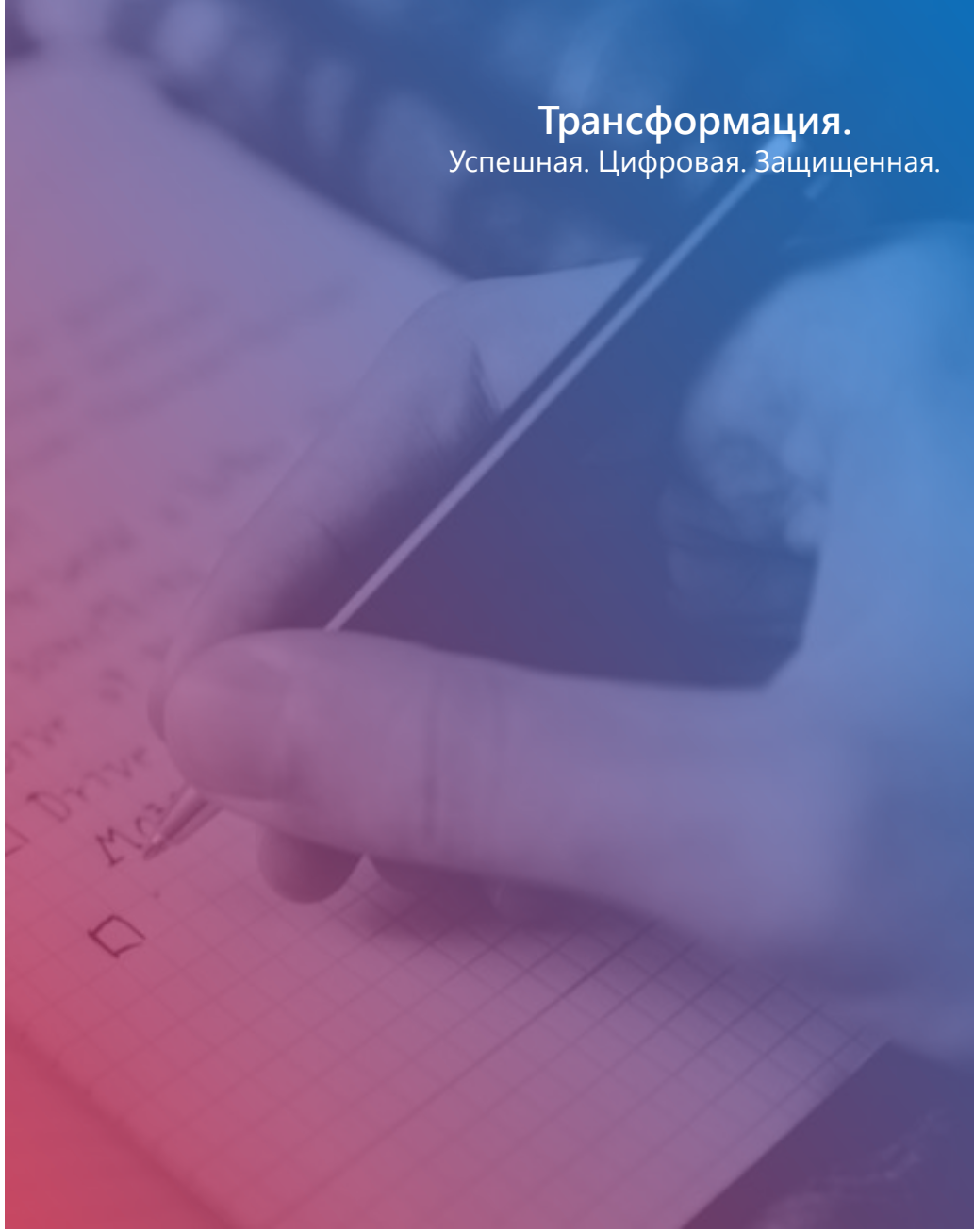
Целенаправленные угрозы (APT)
(Угрозы «нулевого» дня, бесфайловые атаки, незаметное присутствие злоумышленника, горизонтальное перемещение и т.д.)

Бот-сети (Botnets)
(Emotet, Trickbot, Dridex, Roboto)

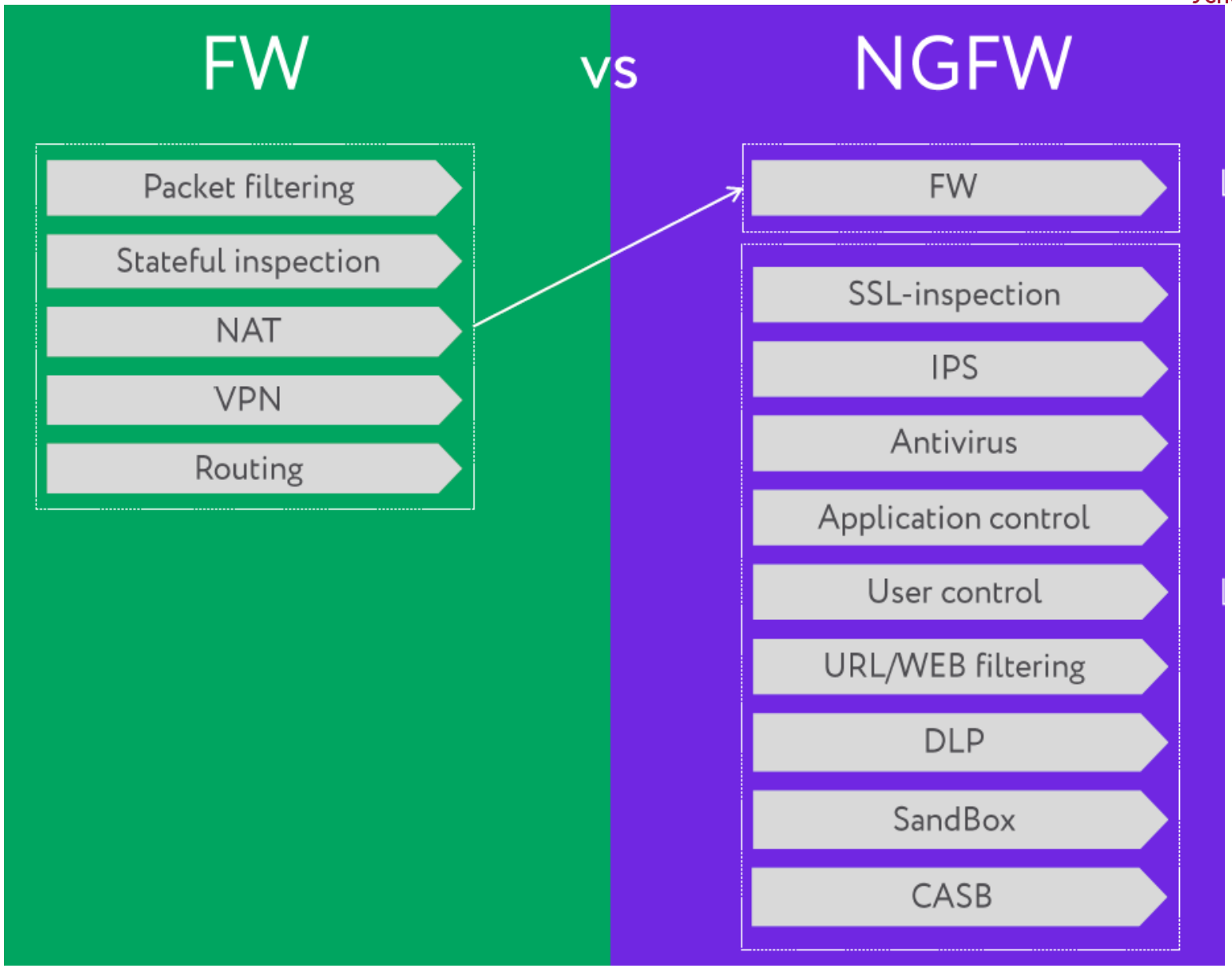
Проблематика

Риски при отсутствии функционального решения

- **Проникновение** и свободное перемещение злоумышленника по сетевой инфраструктуре
- **Распространение вредоносного ПО**
- **Неконтролируемый доступ** к обрабатываемой информации
- **Риск утечек** чувствительных данных
- **Несоблюдение требований** стандартов и нормативных правовых актов в области защиты информации



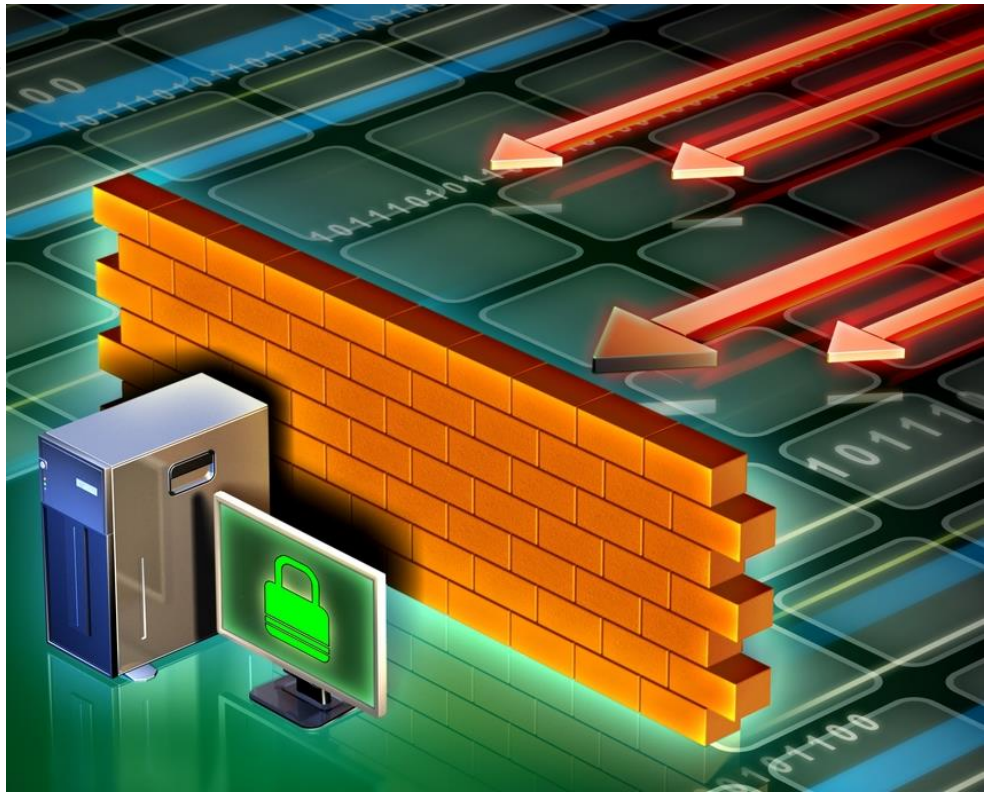
Не все МСЭ одинаково полезный



Основные решаемые задачи

Внедрение межсетевого экрана следующего поколения

- **Анализ сетевого трафика** потоковыми средствами проверки.
- **Реализация микросегментации** сети посредством формирования отдельных сегментов для Приложений, а не только групп портов и/или IP-адресов (L3/L4 модели OSI).
- **Контроль, фильтрация и блокировка трафика** на уровне Приложений (L7 модели OSI).
- **Создание правил, политик**, **ролей** регламентирующих взаимодействие с ресурсам сети Интернет.
- **Интеграция** с Active Directory (AD) и другими системами.
- **Организация** защищённого удалённого подключения.



USERGATE - NGFW

О компании UserGate

Трансформация.
Успешная. Цифровая. Защищенная.

2001
запуск первой версии UserGate Proxy

2009
начало разработки первого российского NGFW UserGate

2010
создан внутренний стартап, в рамках которого началась разработка новой платформы

2012
UserGate – резидент Академпарка в Новосибирске

2015
UserGate – резидент Сколково

2016
выпуск нового UserGate как решения класса UTM

2018
создание экспертной лаборатории и начало разработки собственных аппаратных платформ

Сертификация новой платформы по требованиям ФСТЭК России

2019
открытие первого московского офиса UserGate

2020
открытие офиса UserGate в Хабаровске

начало экспансии UserGate с первым отечественным NGFW на рынке ИБ России

реализовано несколько тысяч проектов, в большинстве из которых замещены зарубежные аналоги

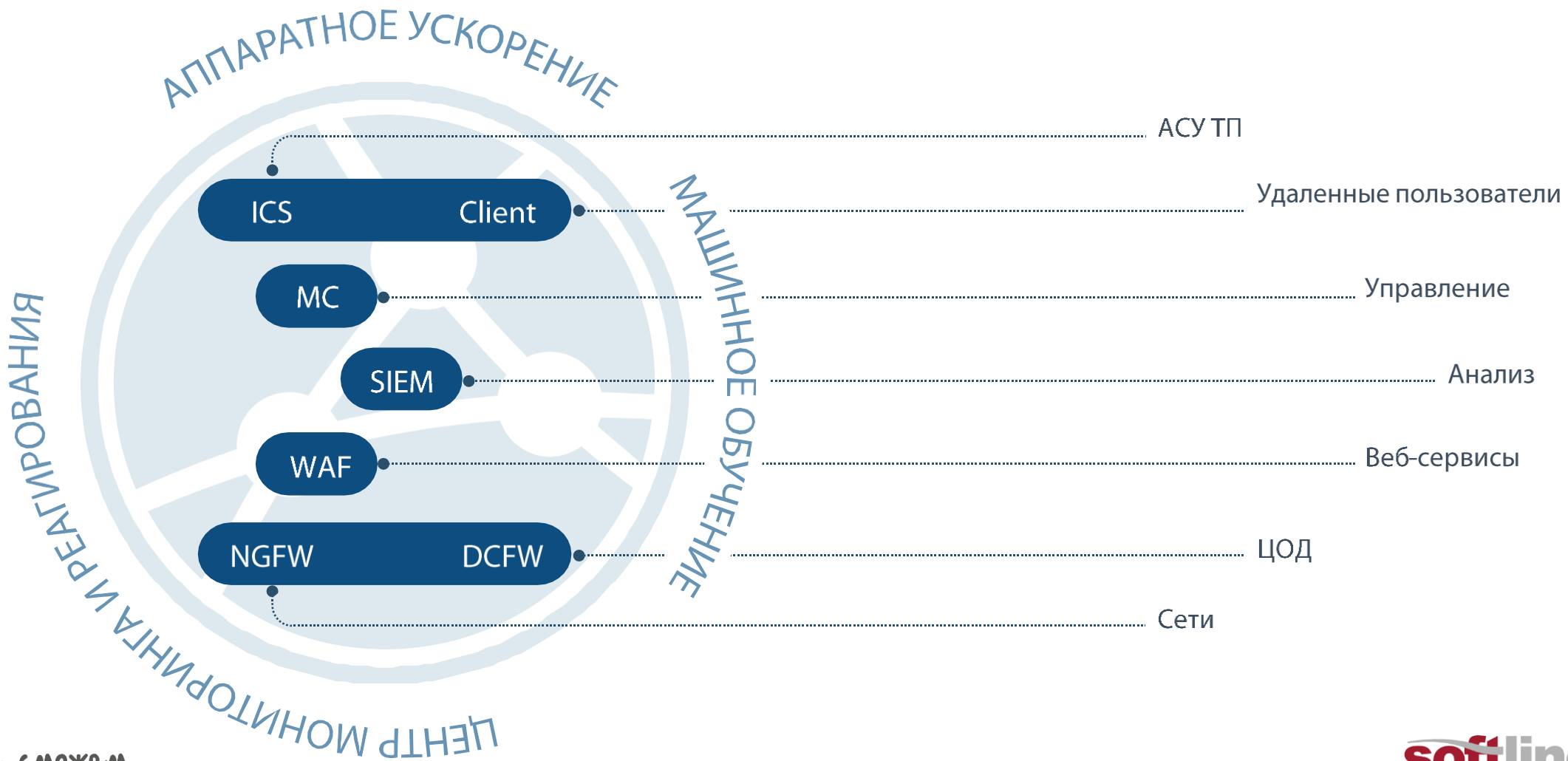
2021
выход на рынок экосистемы безопасности UserGate SUMMA

2022
открытие офиса в Санкт-Петербурге

Usergate SUMMA

Трансформация.
Успешная. Цифровая. Защищенная.

100% видимость событий безопасности



Основный функции UserGate NGFW

Межсетевой экран
(Enterprise Firewall, NGFW)

Защита от угроз
(Threat protection)

Контроль приложений на уровне L7

Интернет-фильтрация
(Internet filtering)

Защита от атак, безопасность дата-центров
(IPS)

Дешифрование SSL

Безопасность почты
(Mail Security)

Операционная система UGOS

Виртуальная частная сеть
(VPN)

Антивирусная защита

Гостевой портал, Captive-портал

Удаленное подключение

Высокая отказоустойчивость и кластеризация
(High Availability and Clustering)

UserGate Management Center

UserGate Log Analyzer

Центр мониторинга и реагирования

UserGate (MRC-UG) – исследование сетевых угроз

Центр мониторинга и реагирования UserGate (MRC-UG) – это команда специалистов по информационной безопасности, которая занимается исследованием сетевых угроз. Командой используются сведения из многочисленных открытых источников, получаются данные от всевозможных платных подписок, баз уязвимостей, а также за счет технологического партнерства с другими компаниями. MRC-UG обладает собственными ловушками (honeypots), на базе которых ведется изучение актуальной противоправной активности в интернете.

Источники информации об инцидентах безопасности

UserGate создает свои сигнатуры на основе:

- Образцов вредоносного трафика.
- Публичных proof of concept на уязвимости.
- Информации от различных CERT.
- Анализа собираемых IoC

Лицензирование

Основная лицензия и дополнительные модули (включая ежегодное продление)

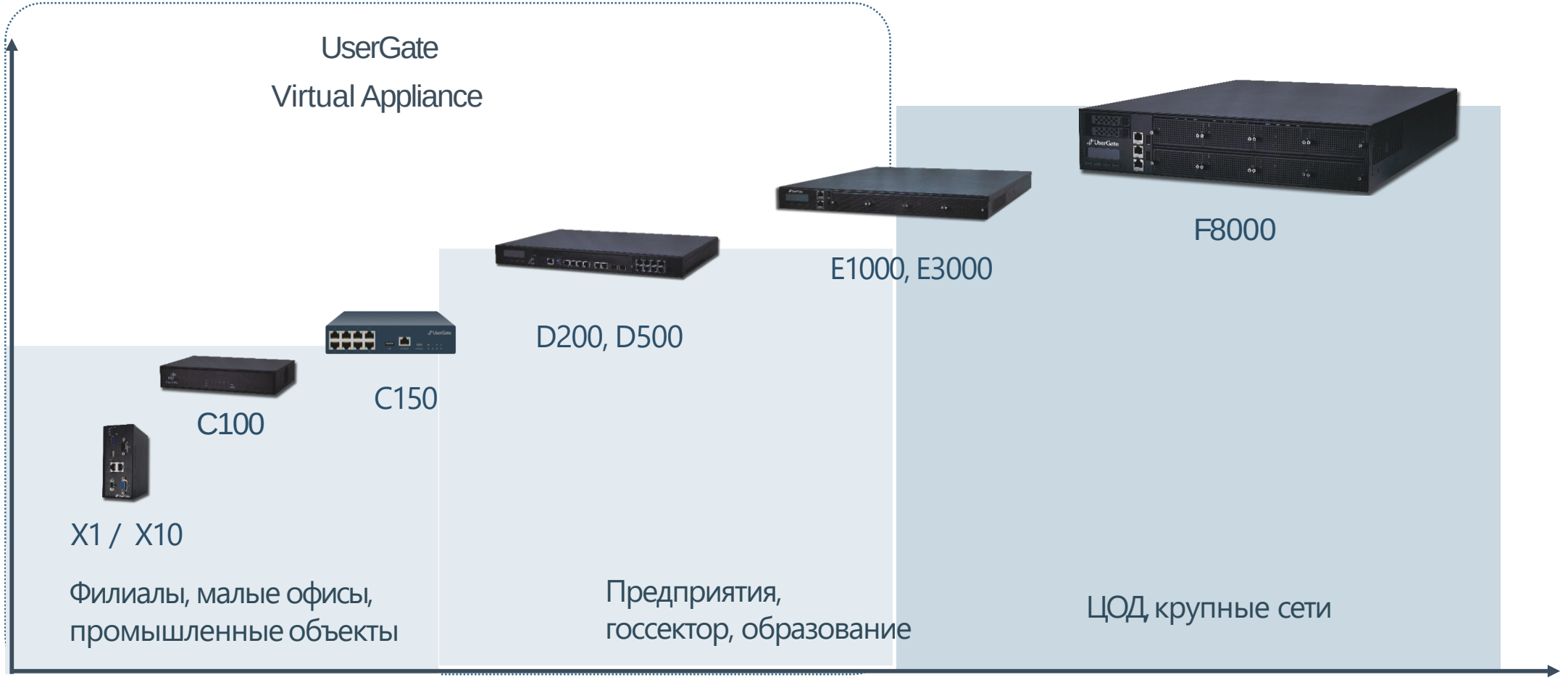
UserGate лицензируется по количеству одновременно подключенных устройств, включая пользователей терминальных серверов, за исключением устройств, чей трафик проходит через UserGate с использованием правил публикации DNAT, Reverse-прокси, веб-портала, защиты почтового трафика.

Основная лицензия приобретается единоразово и действует бессрочно. Включает в себя весь основной функционал, такой как Proxy, NGFW, IDS/IPS и VPN.

Дополнительно ежегодно лицензируются следующие модули:

- **Security Updates.** Включает обновления ПО UserGate, обновления операционной системы, баз сигнатур вторжений и известных приложений (L7), а также техническую поддержку.
- **Advanced Threat Protection.** Включает подписку на использование баз DNS-фильтрации, морфологических словарей, баз категорий сайтов веб-фильтрации и списки Роскомнадзора.
- **Antivirus.** Включает подписку на потоковый антивирус.
- **Mail Security.** Включает подписку на фильтрацию спама

О платформе UserGate

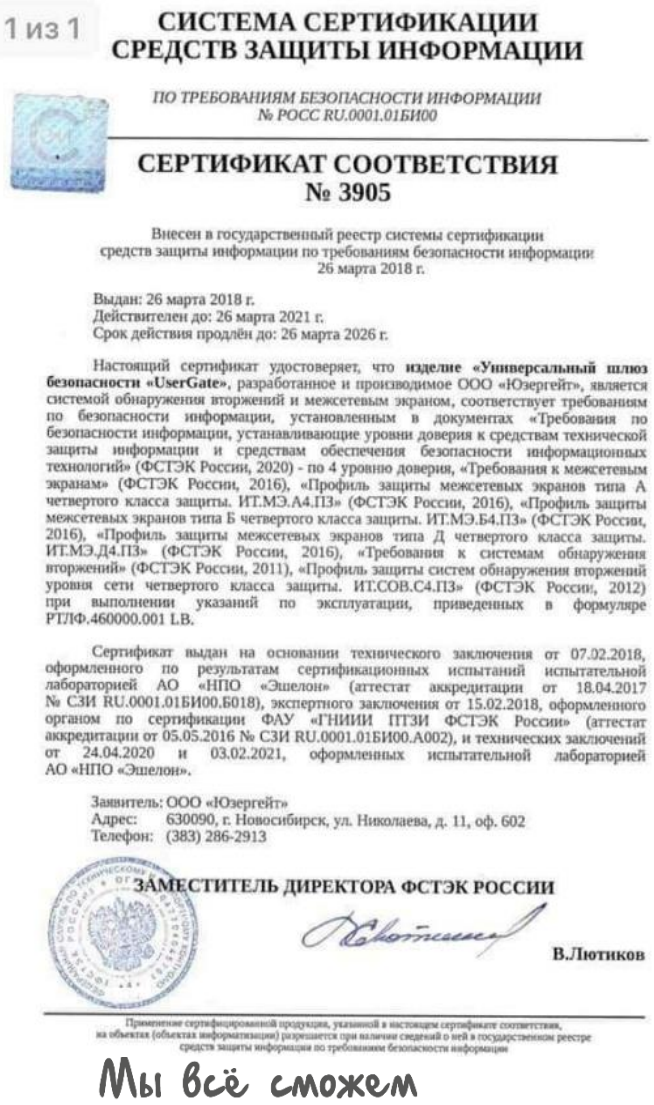


vmware · Xen · KVM · Hyper-V · openstack · VirtualBox

РЕД ВИРТУАЛИЗАЦИЯ · base alt · БРЕСТ · ГОРИЗОНТ-ВС · ROS ПЛАТФОРМА · ViRT

Сертификат ФСТЭК России №3905

Соответствие решения UserGate установленным требованиям



1 из 1

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3905

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
26 марта 2018 г.

Выдан: 26 марта 2018 г.
Действителен до: 26 марта 2021 г.
Срок действия продлён до: 26 марта 2026 г.

Настоящий сертификат удостоверяет, что **изделие «Универсальный шлюз безопасности «UserGate»**, разработанное и производимое ООО «Юзергейт», является системой обнаружения вторжений и межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре РТЛФ.460000.001 ЛВ.

Сертификат выдан на основании технического заключения от 07.02.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), экспертного заключения от 15.02.2018, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технических заключений от 24.04.2020 и 03.02.2021, оформленных испытательной лабораторией АО «НПО «Эшелон».

Заявитель: ООО «Юзергейт»
Адрес: 630090, г. Новосибирск, ул. Николаева, д. 11, оф. 602
Телефон: (383) 286-2913

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ
В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Мы всё сможем

Сертификат ФСТЭК России № 3905, подтверждает соответствие решения UserGate требованиям, установленных в следующих документах:

- Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018) по 4 уровню доверия.
- Требования к межсетевым экранам (ФСТЭК России, 2016).
- Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016).
- Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016).
- Требования к системам обнаружения вторжений (ФСТЭК России, 2011).
- Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012)

Рег. номер ПО:1194 в реестре Минкомсвязи

Проектная деятельность SOFTLINE

Полный цикл реализации проекта

От подбора решения и поставки до внедрения и технической поддержки

- Собственный Производственный блок
- Развитая экспертная команда:
  ИТ, ИБ и Консалтинг
- Собственный Учебный центр
- Собственная система Service Desk, Служба технической поддержки и Сервисный центр
- Гибкая модель предоставления услуг – от внедрения и сопровождения до аутсорсинга

Техническая поддержка и сопровождение

Трансформация.
Успешная. Цифровая. Защищенная.

Сопровождение эксплуатации и функционирования Системы профильными специалистами

Вопросы, связанные с работой ИБ-систем, **решаются силами специалистов Softline** в рамках SLA с прописанной ответственностью Интегратора

Компания Softline становится **единой точкой входа** по всем вопросам, связанным с технической поддержкой ИБ-решений

Инженеры Softline **оказывают консультации** штатным специалистам, чтобы упростить освоение решений инфраструктуры Заказчика

Продукты сетевой безопасности:
Check Point Software Technologies, **Cisco** Systems, **Fortinet**, **Palo Alto** Networks, **UserGate, Код Безопасности, ИнфоТеКС, С-Терра**

Состав услуги:

- **Постановка на сервис**
- Работы с обращениями (**1-я линия**)
- Консультационная поддержка (**2-я линия**)
- Восстановление работоспособности и сессии удалённых подключений (**3-я линия**)

Необходимость подключения штатных сотрудников для самостоятельной выработки обходного решения **отпадает**

Срок постановки на сервис – **3 дня**
Срок оказания технической поддержки – **1 месяц** с момента заключения договора и подтверждения о готовности исполнителя

Стоимость оказания услуг техподдержки – **275 000 руб. + 140 000 руб.** за каждую систему на поддержке после первой

Мы всё сможем

Сетевая безопасность по модели MSSP

Трансформация.
Успешная. Цифровая. Защищенная.

Компоненты сервиса

- помесячная оплата
- предоставление мощностей и лицензий
- выделенная экспертная команда со стороны MSSP-провайдера
- интеграция и постановка на сервис
- техническая поддержка и дальнейшее сопровождение.

Основные преимущества сервисной модели

- отсутствие капитальных затрат со стороны компании
- минимизация временных затрат
- возможность оперативного изменения функционала
- возможность наращивания ресурсов
- гарантия работоспособности сервиса
- выделенная экспертная команда

Пилотное тестирование

Практическая проверка функциональных возможностей и требований к решению

- **Устав** пилотного проекта
- **Программа** и методика испытаний
- **Детализированный отчёт** по результатам тестирования
- **Выдача рекомендаций** по покрытию векторов угроз
- **Демонстрация** функциональных возможностей
- **Качественный переход и реализация** проекта по внедрению

Шкатов Александр
Менеджер группы развития продаж решений информационной безопасности в ЦФО

softline®

Мы всё сможем

Трансформация.

Успешная. Цифровая. Защищенная.