



UserGate

Client

Защищённый доступ
к финансовой инфраструктуре
из любой точки мира



UserGate Client



Защищённый доступ к финансовой инфраструктуре из любой точки мира

- **UserGate Client** — продукт для безопасного и бесшовного подключения удалённых сотрудников к критически важным системам организации с полным соблюдением требований информационной безопасности.

UserGate Client состоит из трёх компонентов:

- **VPN**
удалённый доступ к ИТ-инфраструктуре с пользовательских устройств
- **NAC (комплаенс-проверки)**
контроль безопасного доступа к ИТ-инфраструктуре с использованием концепции нулевого доверия (ZTNA)
- **SIEM-агент**
обогащение данных системы мониторинга за счёт сбора телеметрии

Соответствие требованиям регуляторов, безопасность и скорость передачи данных

Центральный банк РФ

Требования ЦБ РФ к безопасности конечных точек включают в себя защиту как клиентских машин, так и серверов, используемых в финансовых операциях.

Согласно требованиям ЦБ РФ необходимо:

- защищать устройства и информационные системы от вредоносного ПО, а именно — использовать сертифицированные антивирусы в соответствии с политиками безопасности компании
- применять мультифакторную аутентификацию для подтверждения пользователя или устройства
- применять средства защиты от НСД (несанкционированного доступа), контролирующие допуск к системам и данным
- регулярно сканировать инфраструктуру на наличие уязвимостей с целью их последующего устранения, а также вести учёт уязвимостей и своевременно внедрять обновления ПО



Какие требования поможет выполнить UserGate Client

- **№ 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017**
Банковские организации являются субъектами критической информационной инфраструктуры (КИИ) и должны следовать требованиям ФЗ по обеспечению безопасности своих информационных систем
- **Положения Банка России № 716-П, № 787-П и № 779-П**
Субъекты с активами более 500 млрд ₽ должны обеспечивать усиленный уровень защиты от киберрисков и реализовывать требования по операционной надёжности
- **ГОСТ Р 57580.4-2022, ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018, № 152-ФЗ «О персональных данных» от 27.07.2006**
Банковские организации должны обеспечивать идентификацию и аутентификацию, учёт и хранение информации об операциях, устранение уязвимостей и своевременное внедрение обновлений ПО, а также проводить оценку соответствия требованиям информационной безопасности каждые два года
- **Стандарты ЦБ РФ (СТО БР ИББС)**
Банковские организации должны обеспечивать полный контроль доступа, шифрование трафика и детальное логирование всех сессий

Преимущества использования UserGate Client для организаций финансового сектора

Полный контроль доступа, шифрование трафика и детальное логирование всех сессий

Комплексный подход к обеспечению контролируемой защищённой среды для работы из любого местоположения

Нулевые задержки для трейдинга и автоматизированной банковской системы (АБС)

Технология DTLS (Datagram Transport Layer Security) гарантирует безопасность операций без потери скорости, что критически важно для работы с аналитическими сервисами и транзакционными системами

Возможность выявить инсайдеров и защита от внешних угроз

Встроенные компоненты NAC (Network Access Control) и SIEM-агента (Security Information and Event Management) позволяют проверять устройство сотрудника перед доступом к информационным системам и контролировать его действия внутри сети

Снижение затрат на СЗИ

UserGate Client объединяет в себе три важных компонента обеспечения информационной безопасности: NAC, VPN и SIEM-агент. Использование комплексного решения позволяет облегчить работу служб ИБ и снизить стоимость владения СЗИ

Как UserGate Client защищает инфраструктуру

Защищённый канал передачи данных

- **VPN + DTLS**

Применение технологии организации защищённого удалённого доступа (VPN), в том числе с использованием DTLS (Datagram Transport Layer Security), обеспечит передачу финансовых данных без задержек и разрывов сессии

- **Современные протоколы шифрования**

Ни один байт платёжного поручения или клиентской информации не будет использован злоумышленниками в случае перехвата, стабильное шифрование гарантирует целостность передаваемых данных

Строгий контроль доступа по принципу ZTNA (Zero Trust Network Access)

- **Проверка соответствия устройств (комплаенс-проверки)**

Доступ к внутренним информационным системам получает только то устройство, на котором установлено одобренное ПО, обновлены антивирусные базы и включён межсетевой экран (FW)

- **Гибкие политики доступа**

Минимизируйте риски за счёт сегментации: разрешите бухгалтерии доступ только к 1С, а аналитикам — к базам данных и BI-системам

Быстрое обнаружение и реагирование

- **Круглосуточный мониторинг активности**

Телеметрия со всех подключённых устройств позволяет выявлять такие подозрительные действия, как массовое копирование данных или запуск неавторизованных приложений

- **Интеграция с SIEM**

Все события безопасности передаются в UserGate SIEM, позволяя аналитикам быстро реагировать на инциденты

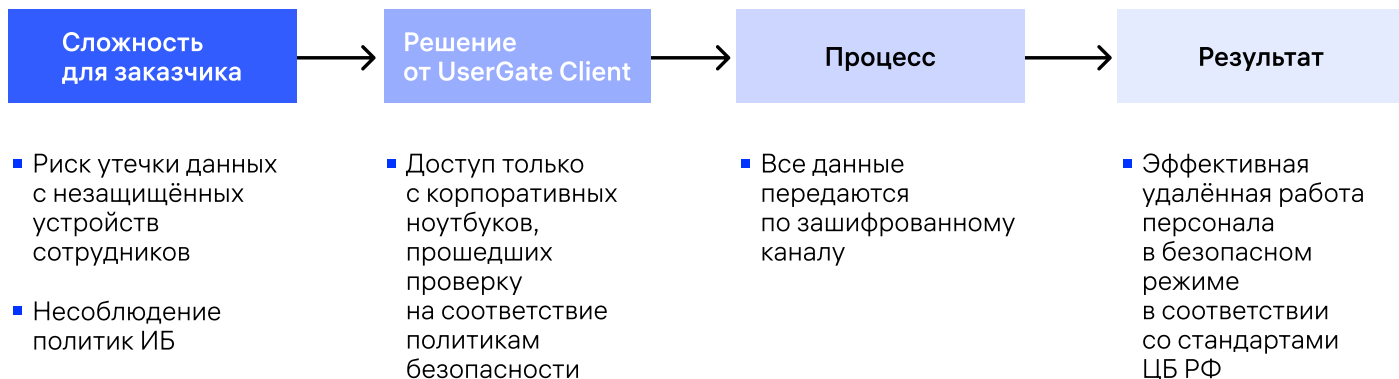
- **Журналирование событий безопасности и сбор телеметрии с конечных точек**

Собранная телеметрия и события безопасности (логи подключения) позволяют определить, кто из пользователей, когда, с какого устройства и к каким системам подключался. Благодаря собранному данным аналитики располагают неизменяемым журналом для отчётности в ЦБ РФ и аудиторам.

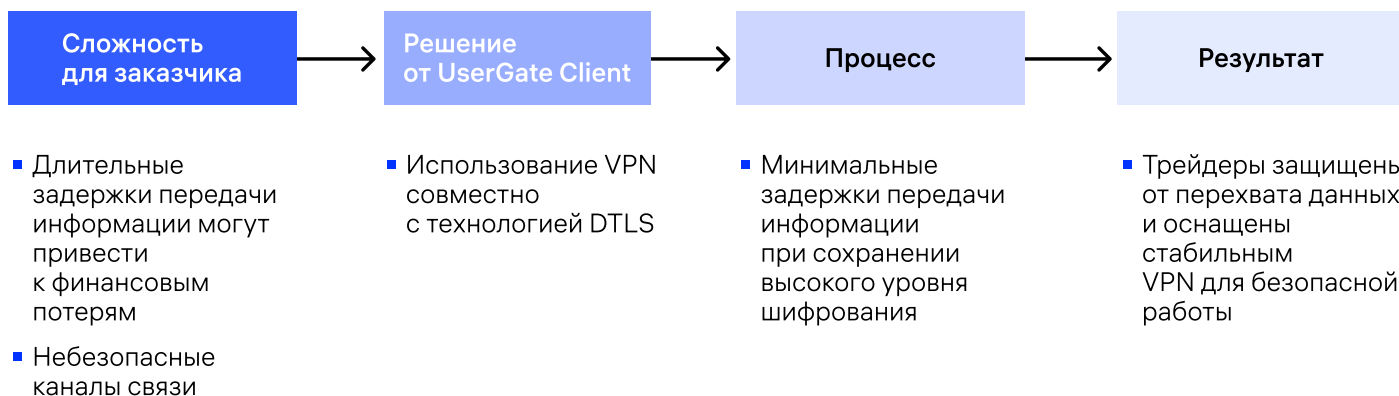


Сценарии применения UserGate Client в финансовой инфраструктуре

Удалённая работа операционистов и сотрудников офиса



Доступ трейдеров к торговым терминалам



Подключение внешних консультантов и аутсорс



Технические особенности UserGate Client

Поддержка ОС: Windows, Linux (VPN)

В 2026 году планируется расширение поддержки ОС семейства macOS, а также ОС семейства Linux, в том числе отечественных

Поддерживаемые технологии:

VPN, протоколы TLS и DTLS, IPsec VPN (IKEv2), Split tunneling, Remote Access VPN

Аутентификация и авторизация

Поддержка LDAP-коннектора, Radius, TACACS+, Kerberos, NTLM, SAML (SSO), 2FA и MFA (TOTP)

Централизованное управление

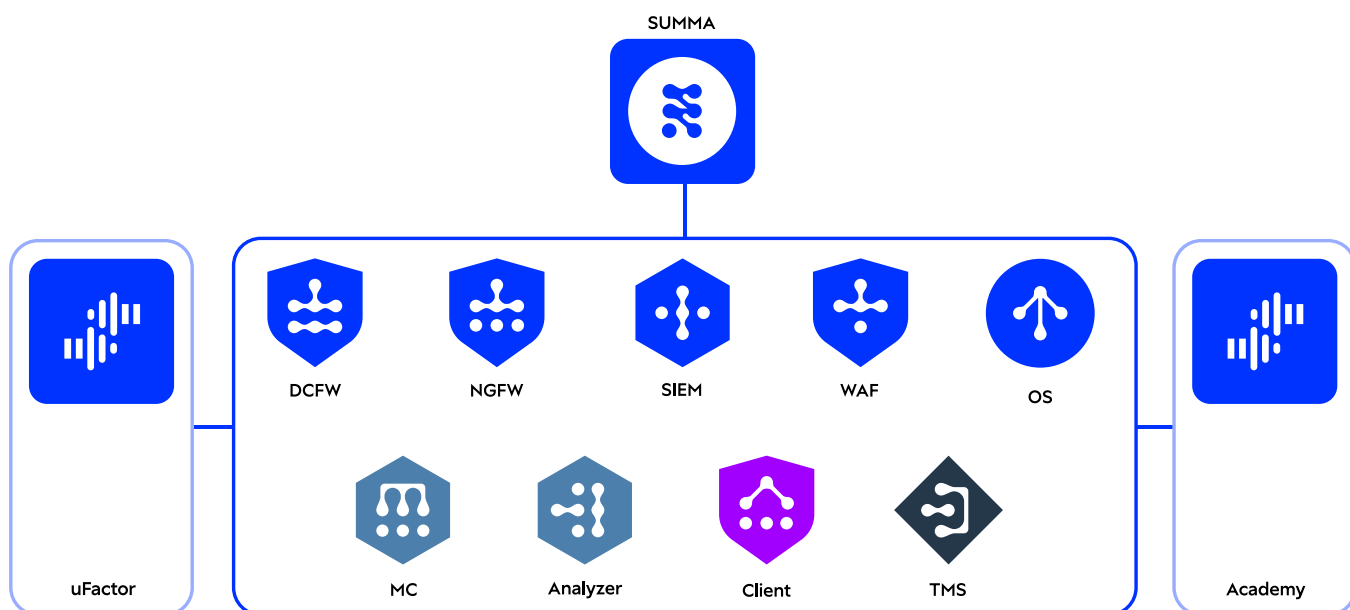
Управление политиками, пользователями и устройствами осуществляется через единую консоль UserGate Management Center

Совместимость

UserGate Client работает в связке с продуктами экосистемы UserGate SUMMA: с UserGate NGFW и UserGate Management Center — для сбора логов и событий информационной безопасности, с UserGate SIEM и UserGate LogAn — для их хранения.



Интеграция с продуктами экосистемы безопасности UserGate SUMMA



- Для централизованного управления из единой точки парком рабочих станций используется режим подключения UserGate Client к UserGate Management Center. В этом режиме UserGate Client сообщает администратору экосистемы UserGate SUMMA данные о состоянии конечных устройств, включая информацию о запущенных приложениях, обновлениях, версиях ПО, загрузках процессора, критических событиях на устройстве, журналах различных сервисов и других параметрах
- Телеметрическая информация, журналы Windows и другие данные о безопасности конечных устройств, полученные от UserGate Client, передаются в систему мониторинга UserGate SIEM и могут быть использованы для автоматического реагирования на угрозы безопасности
- Интеграция UserGate Client с UserGate NGFW, Management Center и SIEM позволяет гибко проводить централизованную настройку большого количества конечных точек, обеспечивать защиту компьютера и соблюдать политики корпоративной безопасности при выходе за защищённый периметр организации

Взять на тест UserGate Client



Контактная информация:

Телефон: 8 800 500-40-32
Клиентам: sales@usergate.com
Партнерам: partner@usergate.com
Маркетинг: marketing@usergate.com

Полезные ресурсы UserGate:

