UserGate

Решения UserGate для медицинских учреждений

UserGate

Проблемы кибербезопасности в медицине

Во 2 квартале 2021 года доля атак на медицинские организации составила 10% от общего числа инцидентов, а в сегменте шифровальщиков-вымогателей 14%. В некоторых случаях кибератаки привели к человеческим жертвам из-за невозможности оказать неотложную помощь.

Поэтому для любой медицинской организации важно не только построить комплексную систему информационной безопасности, обеспечивающую соответствие требованиям регуляторов, но и своевременно обнаруживать и предотвращать угрозы информационной безопасности, не допуская утечек информации и остановки деятельности медицинских информационных систем.

Защита медицинских информационных систем

В качестве основных законов, регулирующих безопасность информации в медицинской сфере, выступают 152-ФЗ «О персональных данных», 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (если медучреждение является субъектом КИИ).

Технические требования и ограничения при работе с медицинскими данными определены в следующих нормативно-правовых актах:

- Постановление Правительства РФ №1119, устанавливающее для данных о здоровье человека самый высокий уровень защиты;
- Приказы ФСТЭК России №17 и №21, которые содержат детальные перечни организационных и технических мер защиты информации;
- Приказ Минздрава №911н, дополняющий требования к информационным сетям медорганизаций (в частности, запрет на допуск иностранной продукции; использование несертифицированных СЗИ, размещение данных за рубежом);
- Постановление Правительства РФ №447, применяется для интегрированных с МИС информационных систем;
- Постановление Правительства РФ №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

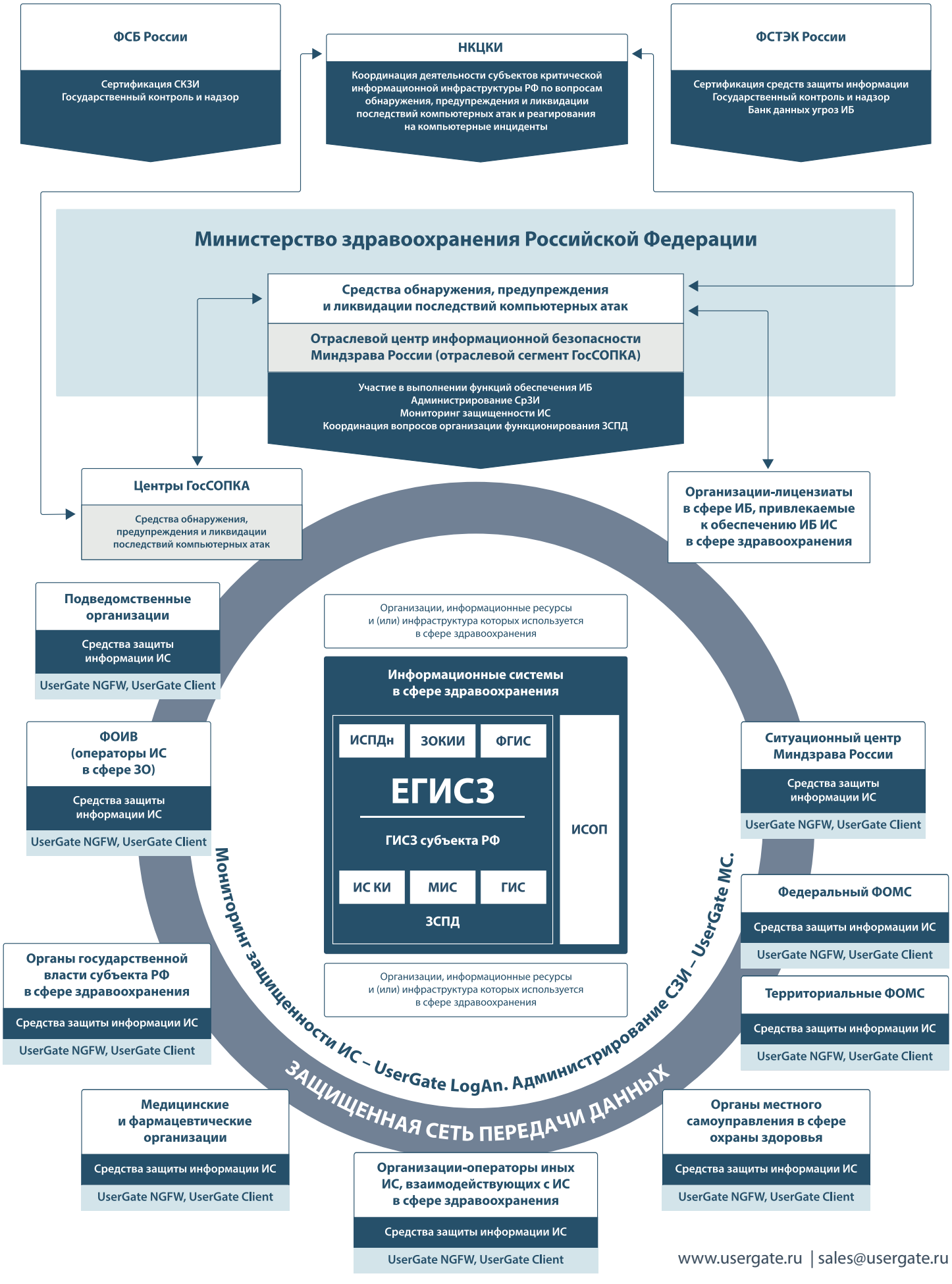
Решения компании UserGate удовлетворяют повышенным требованиям по информационной безопасности для медицинских учреждений. В комплексе продуктов защиты информации UserGate SUMMA центральным компонентом является межсетевой экран нового поколения UserGate.

Соответствие требованиям	
Используемые в медучреждениях СЗИ должны быть сертифицированными ФСТЭК России	**UserGate NGFW сертифицирован ФСТЭК России по требованиям к межсетевым экранам и средствам обнаружения вторжений (4 класс защиты)**
СЗИ должны находиться в реестре российского ПО	**UserGate NGFW внесён в реестр российского ПО (№ 1194)**
Необходимо соблюдать требования ФСТЭК России к обеспечению безопасности информационных систем	**UserGate NGFW выполняет требования по межсетевому экранированию и обнаружению вторжений в аттестованных информационных системах**

www.usergate.ru | sales@usergate.ru

UserGate

Решения экосистемы продуктов UserGate SUMMA можно использовать в качестве средств защиты информационных систем (ИС) в единой системе обеспечения информационной безопасности в сфере здравоохранения по схеме ФГБУ «ЦНИИОИЗ» Минздрава России.



www.usergate.ru | sales@usergate.ru

UserGate

Единое устройство безопасности

Важная особенность UserGate NGFW – многофункциональность, сосредоточенная в едином корпусе. Для выполнения требований по информационной безопасности нужно установить всего одно устройство.

Межсетевые экраны нового поколения UserGate предоставляют многочисленные возможности по управлению функциями безопасности, обеспечивают прозрачность использования интернет-доступа пользователями, устройствами и приложениями.

Работа функций безопасности решения основана на постоянном взаимодействии с центром безопасности UserGate, что позволяет поддерживать минимальное время реакции на известные и неизвестные угрозы. Разработчики UserGate обладают уникальным и специфическим опытом по работе с интернет-ресурсами и угрозами, особенно актуальными для русскоязычного сегмента интернета.

C150

D200 и D500

E1000 и E3000

F8000

www.usergate.ru | sales@usergate.ru

UserGate

Медицинская организация — субъект КИИ

Если медицинская организация является субъектом критической информационной инфраструктуры, и одной из её информационных систем присвоена категория значимости объекта КИИ – необходимо выполнять дополнительные требования информационной безопасности.

В частности, обеспечить выполнение состава мер, устанавливаемых приказом ФСТЭК России №239:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений и компьютерных атак (СОВ);
- защита информационной системы и ее компонентов (ЗИС);
- реагирование на компьютерные инциденты (ИНЦ).

Сертифицированный межсетевой экран нового поколения UserGate позволяет выполнить требования, предъявляемые ФСТЭК России к значимым объектам критической информационной инфраструктуры.

Защита центров обработки данных

Медицинские информационные системы, объединяющие один или несколько регионов, для своего размещения требуют значительных серверных мощностей, которые аккумулируются в специализированных центрах обработки данных. По требованиям законодательства центры обработки данных должны обеспечивать 1 уровень защищённости.

Центры обработки данных регулярно становятся объектами целенаправленных атак, подвержены угрозам распространения вредоносных программ и уязвимостям используемого программного обеспечения.

Решение UserGate для центров обработки данных обеспечивает автоматизированную реакцию на инциденты в соответствии с концепцией SOAR (Security Orchestration, Automation and Response), а также оповещает администраторов об инцидентах безопасности.

Платформы UserGate серии E, F поддерживают высокую доступность, отказоустойчивость и масштабируемость. Встроенные SFP-порты позволяют принимать большой поток трафика, а мощные процессоры анализируют и очищают его. UserGate NGFW способен обеспечить защиту от внешних вторжений и вирусов даже при высокой сетевой нагрузке.

UserGate

Безопасность как услуга

UserGate NGFW можно развернуть в среде виртуализации в качестве виртуальной машины на инфраструктуре заказчика или в облаке по модели SECaaS (UserGate as a Service). При этом производительность будет зависеть только от объёма выделенных ресурсов, без дополнительных лицензионных ограничений.

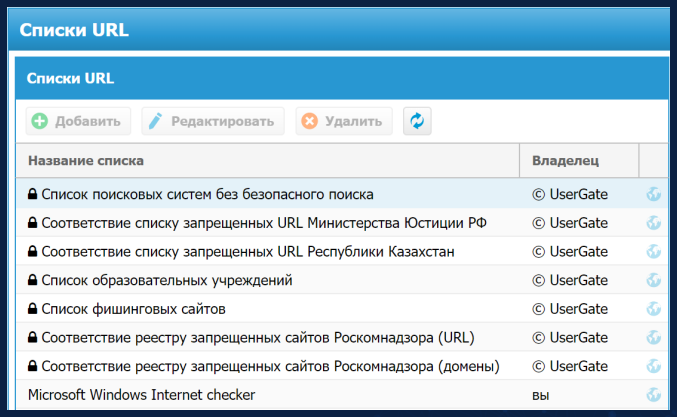
Операционная система UGOS

В основе UserGate NGFW – собственная операционная система UGOS. Полный контроль над кодом, использование собственных модулей позволяют обеспечивать высокое качество работы продукта, а также его скорейшее развитие и адаптацию для самых сложных проектов.

Интернет-фильтрация

Интернет-фильтрация повышает безопасность сети передачи данных, так как позволяет контролировать пользовательский трафик, блокирует загрузки вредоносного ПО, ограничивает посещение пользователем нежелательных ресурсов.

UserGate NGFW блокирует контент не только по адресу сайта из списка (предоставленного Роскомнадзором или созданного вручную). Проводится дополнительный контентный анализ содержимого страницы и морфологический разбор отдельных слов. В результате каждому ресурсу присваивается категория, если URL в списке нежелательных, он будет заблокирован для пользователя.



UserGate NGFW может обеспечить также:

- блокировку рекламы;
- принудительное включение безопасного поиска для поисковых систем (при этом не выводится нежелательный контент);
- блокировку приложений популярных социальных сетей.

www.usergate.ru | sales@usergate.ru

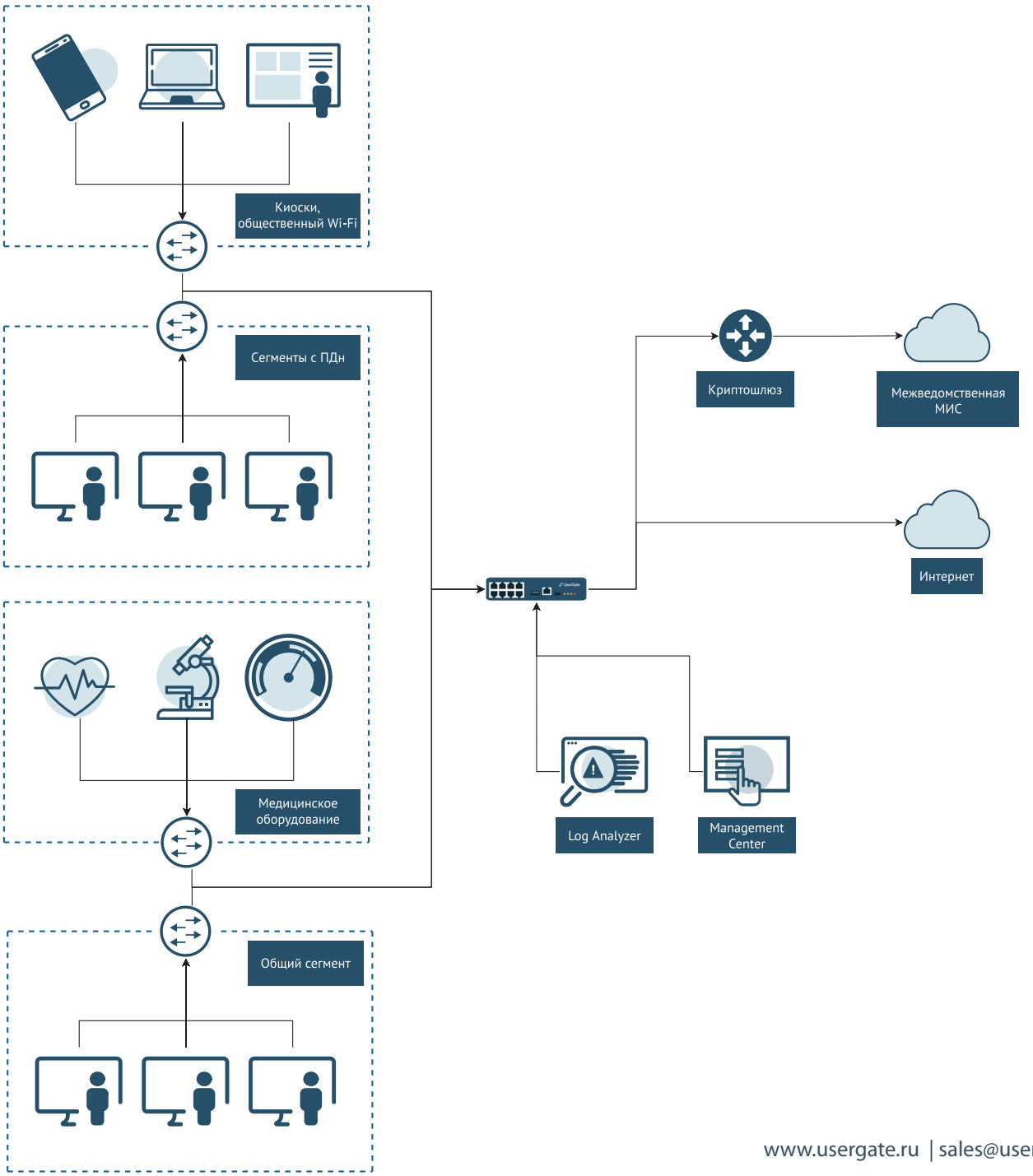
UserGate

Защита медицинских информационных систем

UserGate NGFW сочетает в себе все необходимые функции для построения комплексной системы обеспечения информационной безопасности:

- межсетевое экранирование (L3/L7);
- система обнаружения и предотвращения вторжений (собственный высокопроизводительный движок);
- контроль электронной почты;
- обнаружение вредоносного ПО и антивирусная защита;
- контроль мобильных устройств (для их безопасного использования в качестве рабочих станций);
- SSL VPN;
- гостевой портал (Captive Portal);
- поддержка кластерных конфигураций для отказоустойчивости и распределения нагрузки;
- защита медицинского оборудования (разбор технологических и медицинских протоколов, блокировка определённых команд).

Эти возможности призваны предотвратить растущее количество атак, происходящих на 3–7 уровнях сетевой модели OSI.



UserGate

UserGate SUMMA
Экосистема продуктов кибербезопасности

Анализ инцидентов ИБ

Задачу глобального мониторинга систем безопасности в медицинских информационных системах решает UserGate Log Analyzer, он осуществляет сбор, обработку и хранение данных со всех устройств UserGate. На основании полученных данных осуществляется глубокий анализ произошедших событий безопасности, что, в том числе, необходимо для соответствия современной концепции Security Automation, Orchestration and Response.

Высокая скорость обработки трафика позволяет на основе этого анализа автоматически осуществлять адекватную реакцию на самой ранней стадии.

UserGate Log Analyzer развертывается отдельно от шлюза безопасности, что повышает надежность и обеспечивает масштабируемость системы.

Управление безопасностью медицинской организации

UserGate Management Center – единая консоль управления всеми устройствами UserGate, из которой администратор может выполнять мониторинг, применять необходимые настройки, создавать политики, применяемые к группам устройств для обеспечения безопасности сети.

Безопасность рабочих станций

UserGate Client обеспечивает функции межсетевого экранирования и контентной фильтрации на рабочих станциях, осуществляет сбор информации о различных событиях и метриках операционной системы, работая совместно с UserGate LogAn, позволяет эффективно реагировать на угрозы информационной безопасности.

Телефон: **8 (800) 500-40-32**

Клиентам: **sales@usergate.ru**

Партнерам: **partner@usergate.ru**

SC Magazine Awards 2014 Finalist Honored in the U.S.

SC Magazine Awards 2015 Europe Winner

2015 Computing Security Awards ★ Finalist ★

SC Awards 2017 finalist

Лучшие IT-решения для повышения эффективности ЦИФРОВЫЕ ВЕРШИНЫ

SC Awards 2020 finalist

Sk ИТ