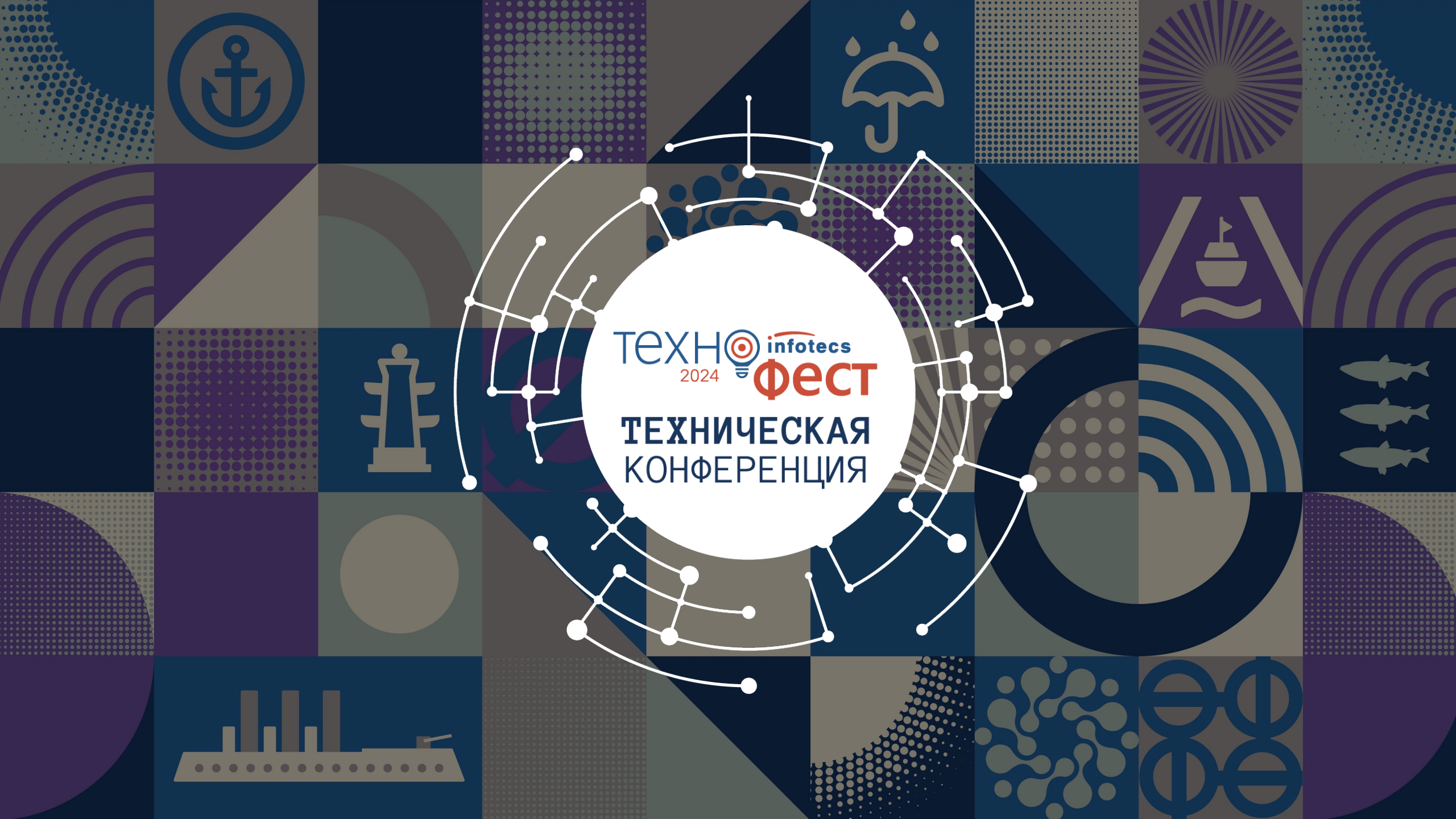

ТЕХНО
2024
infotecs
ФЕСТ
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

Современные подходы в организации сетевого доступа

Калита Александр Викторович
Директор департамента

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

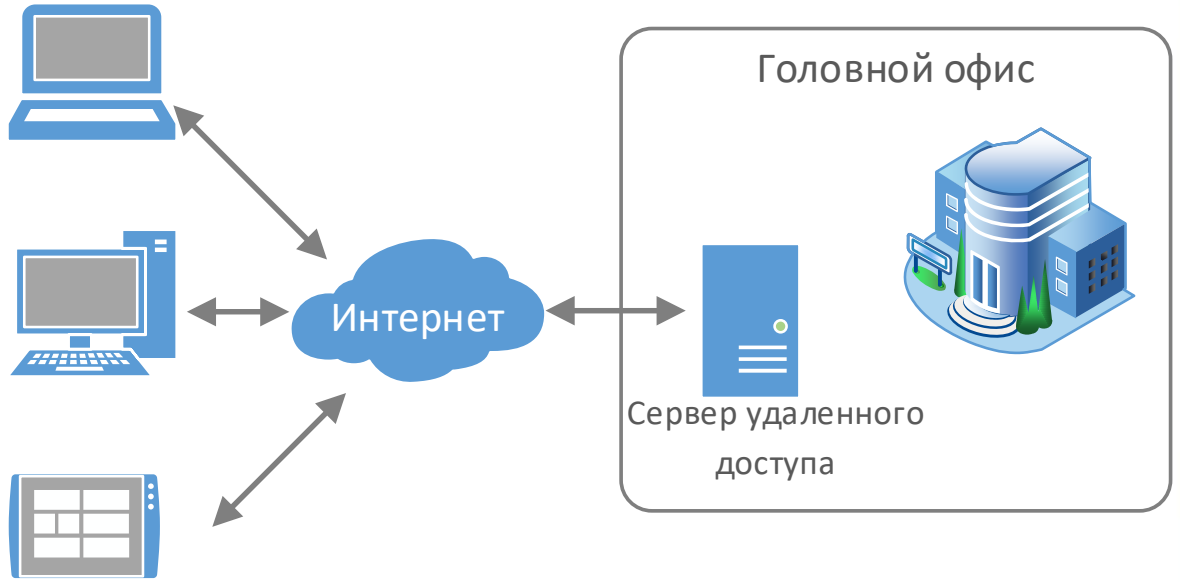
План доклада

1. Удаленный доступ, основные подходы к его реализации
2. Защищенный удаленный доступ
3. Принципы сетевой безопасности
4. Выводы

Удалённый доступ

Системы удаленного доступа (Remote Access)

– это ряд технических решений, обеспечивающих «прозрачное» подключение к сети для удаленных пользователей или малых сетевых сегментов, как правило, расположенных за пределами локальной сети организации.



Способы организации удалённого доступа

1. Использование корпоративного компьютера дома
2. Подключение к компьютеру через Remote Desktop Protocol (RDP)
3. Терминальный сервер
4. Virtual Desktop Infrastructure (VDI)

Использование корпоративного компьютера дома

Кому подойдет	• Небольшим компаниям
Преимущества	• Быстро
Недостатки	• Низкий уровень безопасности данных • Отсутствие контроля по физическому доступу к устройству

Подключение к компьютеру через RDP

Кому подойдет	• Небольшим компаниям
Преимущества	• Быстро • Средний уровень безопасности данных
Недостатки	• Ограничения в работе с графическим контентом

Терминальный сервер

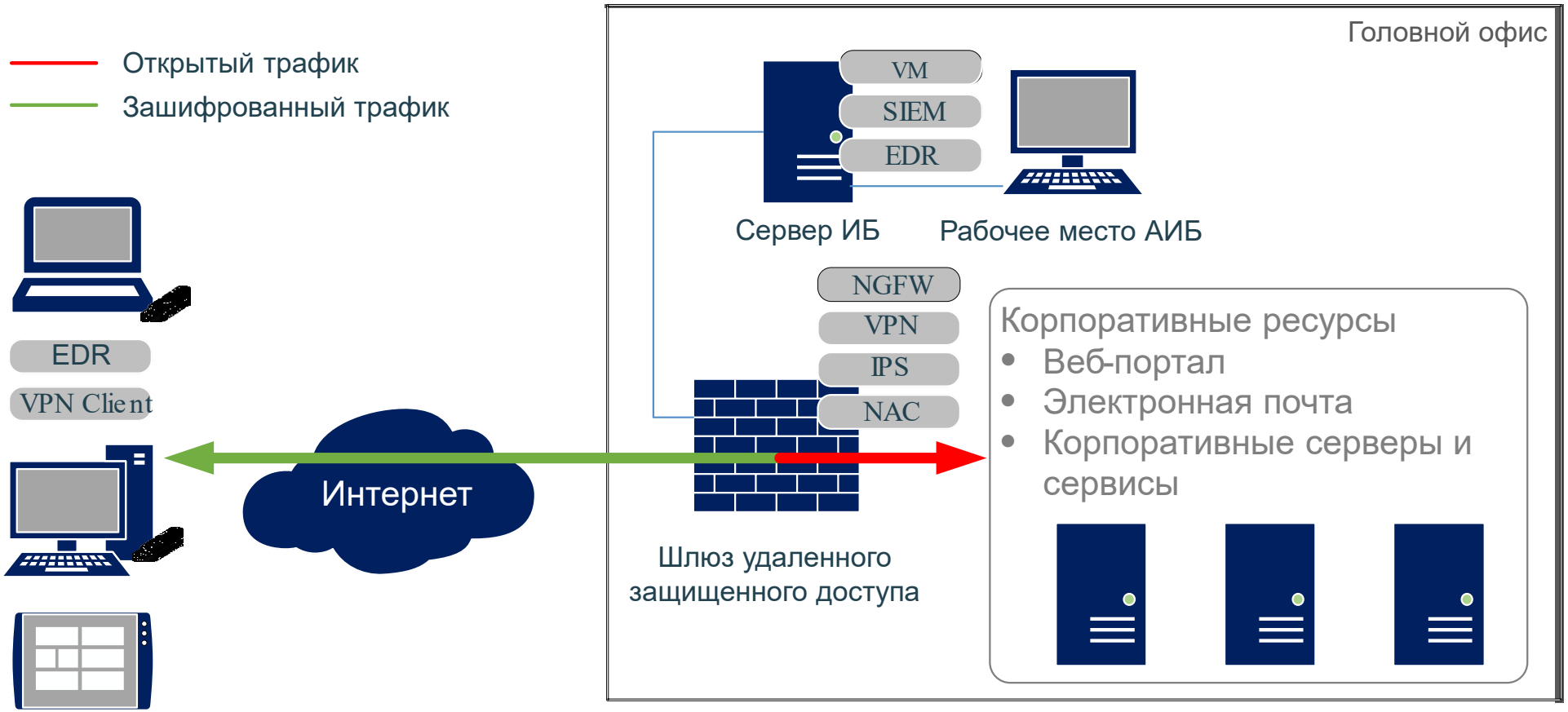
Кому подойдет	• Компаниям любого масштаба
Преимущества	• Средний уровень безопасности данных
Недостатки	• Затраты на приобретение оборудования и программного обеспечения • Требуется время на проведение работ • Ограничения в работе с графическим контентом и некоторыми приложениями

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

VDI

Кому подойдет	• Компаниям любого масштаба
Преимущества	• Высокий уровень безопасности данных • Нет ограничений в работе с графическим контентом
Недостатки	• Большие затраты на приобретение оборудования и программного обеспечения • Требуется время на проведение работ

Защищённый удалённый доступ



Статистика атак на удалённый доступ

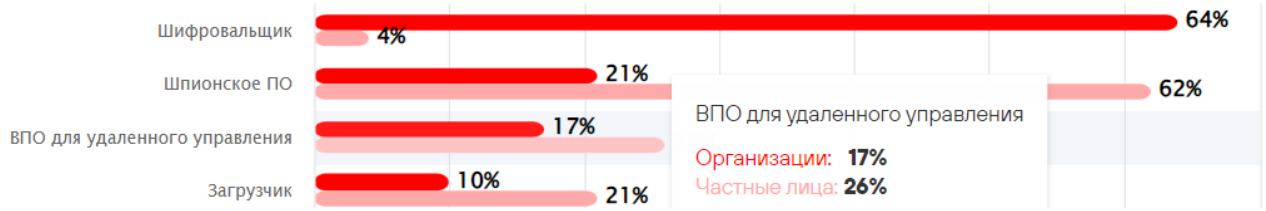
Sophos:

- В 2023 в 90% атак способом получения первоначального доступа выступал RDP.
- В дальнейшем с помощью удаленного доступа по корпоративной сети распространялось различное ВПО.

Отчет CISOCLUB

Positive Technology:

- По популярности ВПО для удаленного управления занимает 3 место, среди остальных вирусов



Актуальные киберугрозы: II квартал 2023 года

HP Wolf Security:

- Эпидемия RAT. За III квартал 2023г. Возросло использование RAT в легитимных файлах (Excel, Powerpoint).
- Parallax RAT сместился с 46-ого на 7-ое место ВПО по популярности.

Threat Insights Report

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

Меры обеспечения защищённого удалённого доступа

Организационные меры

- Дополнительное обучение пользователей
- Информирование сотрудников о необходимости повышения бдительности и соблюдения цифровой гигиены
- Обеспечение комфортных условий работы

Технические меры

- Двухфакторная аутентификация
- Регулярное сканирование сети на предмет уязвимостей
- Организация доступа к внутренним ресурсам через VPN
- Безопасная публикация необходимых веб-ресурсов (WAF)
- Терминальный доступ к конкретным приложениям и т.д.

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

Принципы сетевой безопасности

- Контроль доступа удаленных сотрудников к корпоративным ресурсам
- Назначение прав доступа пользователей в зависимости от устройства с которого осуществляется доступ
- Контроль устройств пользователей с которых осуществляется удаленный доступ на соответствие корпоративным стандартам безопасности
- Усиленная авторизация и контроль действий удаленных пользователей

Использование решений для организации ЗУД

Network Access Control

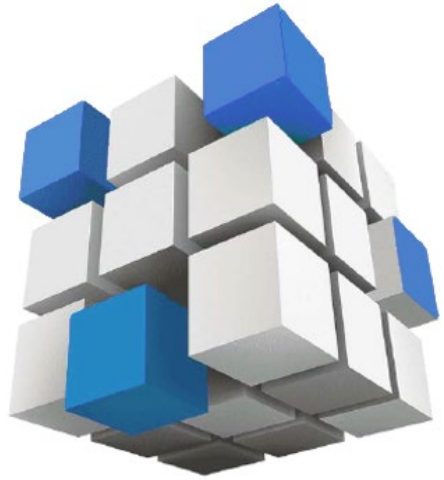
Разграничение и контроль доступа сети

Network Assurance

Контроль конфигураций АСО и топологии сети

Integrity Check

Контроль целостности и проверки соответствия хостов



Vulnerability Control

Анализ уязвимостей и построение векторов атак

Firewall Assurance

Оптимизация и настройка межсетевых экранов

Change Manager

Автоматизация управления межсетевыми экранами

Network Flow Analysis

Анализ статистики сетевого трафика

Netflow, sFlow, IPFIX и NetStream

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

Выводы

Удаленный доступ – это не только удобно, но и необходимо в современных условиях.

Чтобы сохранить и не потерять, необходимо защищать удаленный доступ.

Мы сделали это для себя, сделаем и для вас!

Спасибо
за внимание!

GIS ГАЗИНФОРМ СЕРВИС
20 лет вместе