Комплексный подход к организации **удаленного доступа**

Информзащита
Системный интегратор

В современном мире недостаточно просто настроить VPN для удаленного подключения сотрудника к ресурсам компании. Само по себе решение этой задачи позволяет решить проблему организации дистанционной работу, но существенно понижает защищенность информационных ресурсов в связи с появлением в сети новых рабочих станций.

Через существующую на момент подключения уязвимость новой станции потенциальный злоумышленник достаточно просто попадает в сеть компании.

Поэтому для удаленного доступа требуется комплексный подход к обеспечению безопасности:

Обеспечить возможности удаленного подключения к ресурсам компании

Данная задача решается установкой **VPN-шлюза** на границе сети, а также установкой специализированного **VPN-клиента** на рабочую станцию сотрудника. Практически во всех современных межсетевых экранах Next Generation Firewall (NGFW) имеется данная возможность.

Такие решения присутствуют у следующих вендоров:

Palo Alto Networks Inc

Check Point Software Technologies Ltd

Fortinet Inc

Если необходимо использовать шифрование на основе алгоритма ГОСТ – данное решение моет быть реализовано на основе следующих вендоров:

Infotecs (VipNet)

Код безопасности (АПКШ «Континент»)

S-terra

Обеспечить безопасности рабочей станции и мобильных устройств

Решения по защите конечных точек осуществляют комплексную защиту рабочей стации от несанкционированного доступа. Данный класс решений обеспечивает защиту путем реализации следующих функций:

- **идентификация и аутентификация пользователя**
- **защита удаленного рабочего места средствами персонального межсетевого экрана**
- **организация замкнутой программной среды**
- **антивирусная защита**
- **контроль целостности**
- **обнаружение вторжений**

Примерами таких решений могут быть продукты следующих вендоров:

Kaspersky Endpoint Security для бизнеса от ЛК

Trend Micro Smart Protection от компании Trend Micro Inc

Symantec Endpoint Security от Broadcom Inc

При необходимости использовать сертифицированное решение:

КОД БЕЗОПАСНОСТИ

Код Безопасности

Решение реализовано на основе **Secret net Studio** с модулями персонального межсетевого экрана, средствами обнаружения вторжений и антивирусной защиты.

Решения по защите мобильных устройств, позволяют обеспечить комплексную защиту и безопасность корпоративных данных, при организации рабочего процесса с использованием мобильных устройств. Данный класс решений включает:

- **защиту корпоративных данных на мобильном устройстве**
- **контроль доступа к корпоративным документам**
- **защита от веб-угроз**
- **мониторинг системных событий и действий пользователей**

Такие решения есть у следующих вендоров:

Check Point Capsule от Check Point Software Technologies Ltd

WorksPad от «МобилитиЛаб»

Контроль соответствия уровня защиты удаленной рабочей станции принятым в компании уровням защиты

Функции контроля соответствия уровня защиты удаленной рабочей станции входят в состав решений класса **Next Generation Firewall (NGFW)** и позволяют осуществлять:

- **анализ и контроль защищенности подключаемых по средствам VPN устройств на соответствие корпоративным стандартам безопасности**
- **разграничение доступа пользователя к ресурсам на основе анализа контроля защищенности**

В случае, если в результате анализа будет выявлено несоответствие подключаемой удаленной рабочей станции стандартам безопасности, то возможна как полная блокировка, так и дополнительная авторизация.

Данное решения есть в портфеле следующих вендоров:

Palo Alto Networks

Check Point Software Technologies Ltd

Cisco Systems, Inc

Контроль удаленной сессии

Использование решений для управления привилегированными учетными записями и контроля доступа привилегированных пользователей позволяют обеспечить в системе:

- **единую точку входа привилегированных пользователей**

- регламентацию доступа к привилегированным учетным записям для программных и аппаратных систем и приложений
- ограничение доступа к конкретным ИС или серверам на заданный промежуток времени
- сохранность паролей и возможность их быстрой смены
- контроль привилегированной сессии с возможностью прерывания
- отслеживание выполнения заданных команд в реальном времени
- запись контролируемой сессии для расследования инцидентов
- возможность ретроспективного анализа
- прерывание привилегированной сессии

Вендора и возможные решение:

СКДПУ от АйТи БАСТИОН	CyberArk Privileged Account Security Solution от CyberArk Software	SafeInspect от компании Новые технологии безопасности

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Сервисный центр

+7 495 981 92 22
+7 495 980 23 45 доб.06
support@itsoc.ru
www.itsoc.ru

Центр противодействия кибератакам IZ SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Информзащита
Системный интегратор