

# ViPNet SafePoint 1.5 - новая версия с поддержкой отечественных операционных систем

Кадыков Иван  
Руководитель направления

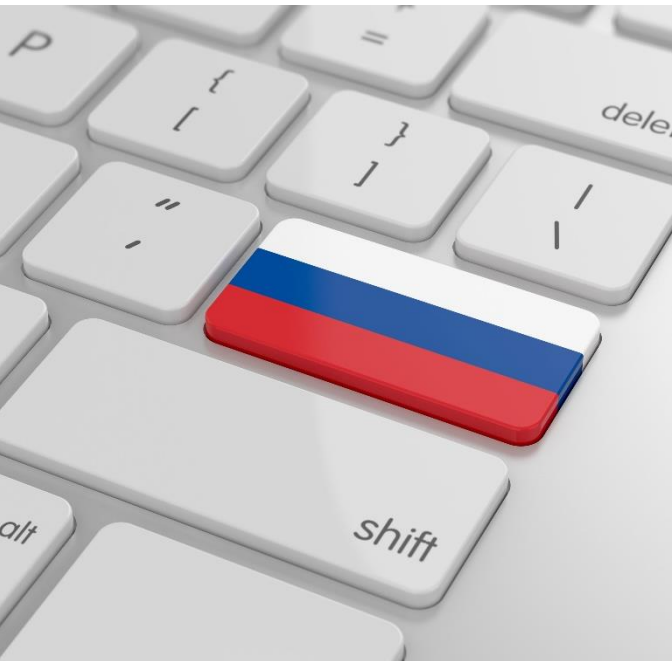
The logo for infotecs, featuring a stylized orange and red arc above the word "infotecs" in a bold, blue, sans-serif font.



The background of the slide is a server room with rows of server racks. The image is overlaid with a semi-transparent blue filter and various digital graphics, including a globe, bar charts, and circular progress indicators. One circular indicator on the left shows '72%' and another on the right shows '82%'. The overall aesthetic is clean, modern, and tech-oriented.

# Вступительное СЛОВО

# Активная фаза перехода на отечественные продукты



- Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
- Многие компании постепенно переходят на \*NIX системы (упор на отечественные)
- 01.11.2022 – Минцифры определили(выбрали) три самых популярных отечественных \*NIX-системы

# Мгновенно Взять и всё заменить?

Задача непростая, но выполнимая!

Не все могут сразу перейти  
на новые ОС из-за:

- нехватки СПО под определённые ОС
- финансовых ограничений
- необходимостью обучения сотрудников

НО! Все стараются!



# Мы активно работаем над ЭТИМ

Все наши продукты, которые устанавливаются на компьютеры пользователей, поддерживают несколько «популярных» отечественных операционных систем







## «Российский Endpoint»

Средство защиты  
от несанкционированного  
доступа

The background is a server room with rows of server racks. Overlaid on this are various digital graphics: a large globe, bar charts, line graphs, and circular progress indicators. One circular indicator on the left shows '72%' and another on the right shows '82%'. The overall color scheme is light blue and white with some orange highlights from a lens flare effect on the left.

# VIPNet SafePoint краткий обзор

# ViPNet SafePoint

## ViPNet SafePoint –

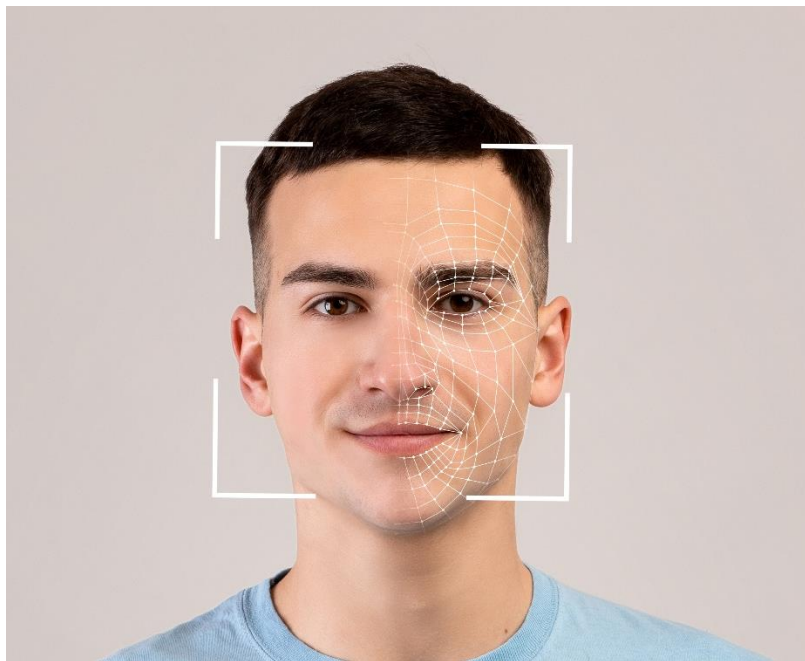
сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС).

**ViPNet SafePoint** устанавливается на рабочие станции и сервера в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам.





# С чего начинается защита от НСД?



Своих пользователей надо знать «в лицо», поэтому:

- **Идентификация и аутентификация пользователей**

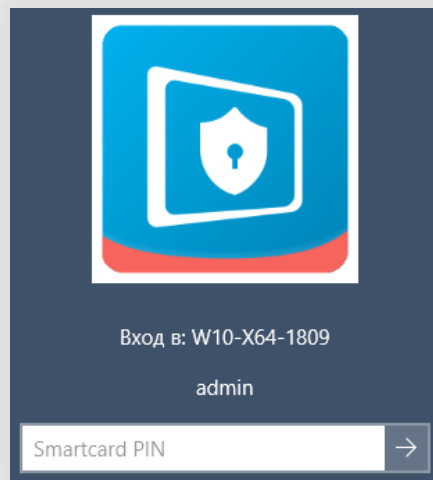
выполняется собственными механизмами

Используем комбинации:

- Логин и пароль
- Логин и идентификатор

# Поддержка USB-токенов и смарт-карт

- JaCarta PKI
- JaCarta PKI/ГОСТ
- JaCarta ГОСТ
- JaCarta 2 PKI/ГОСТ
- JaCarta-2 S
- JaCarta-2 ГОСТ
- JaCarta-2 PRO/ГОСТ
- JaCarta LT
- Rutoken S
- Rutoken Lite
- Rutoken ЭЦП 2.0



# Создание разграничительных политик для пользователя

После прохождения идентификации и аутентификации, необходимо чтобы пользователь:

- Работал только с тем ПО, которое разрешено
- Мог работать только с теми файлами/документами для которых хватает прав(полномочий)
- В системе запускались, только разрешённые процессы
- Не модифицировал(-ись) важные модули



# Разграничительные политики для ПО

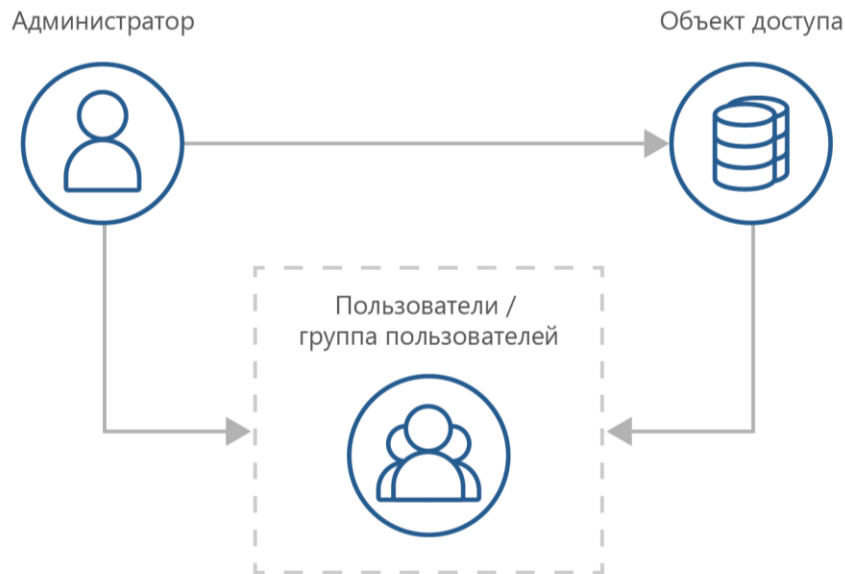


- Контроль службы обновлений операционной системы
- Контроль служб обновлений иностранного ПО
- Обнаружение и запрет запуска подсистемы Windows Installer
- Контроль запуска/исполнения новых файлов и приложений из Temp и AppData

# Разграничение доступа

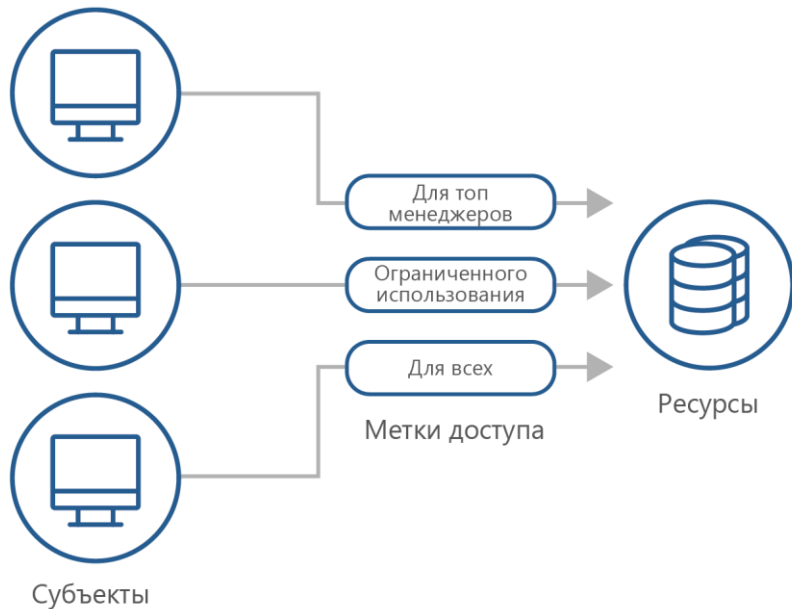
Дискреционный контроль доступа к

- файловой системе (вкл. сменные)
- прямому доступу к диску
- реестру
- принтерам
- службам
- устройствам
- буфер обмена
- виртуальным машинам





# Мандатный контроль доступа пользователей и процессов



Разграничительная политика  
на основе меток безопасности

# Замкнутая программная среда и контроль времени работы

Защита от  
модификации  
запускаемых  
модулей (РПД)

Ограничение  
по каталогам  
запуска  
(РПД)  
%SystemRoot%  
%ProgramFiles  
%

Контроль  
запуска  
скриптов (по  
расширениям  
или хост-  
процессу)

Разрешенные  
процессы  
%SystemRoot%  
%ProgramFiles  
%

Обязательные  
процессы  
(Пользователь  
+ командная  
строка)

Расписание  
работы  
(Процесс +  
День недели,  
Начало,  
Окончание,  
Максимум,  
Аудит)

# Контроль устройств

- Контроль монтирования (подключения) и отключения
- При наличии файловой системы поддерживаются Чтение, Запись, Исполнение, Удаление, Переименование
- Аудит этих событий

USB,  
SATA/ATA/ATAPI,  
PCMCIA,  
CD/DVD/BD, SD

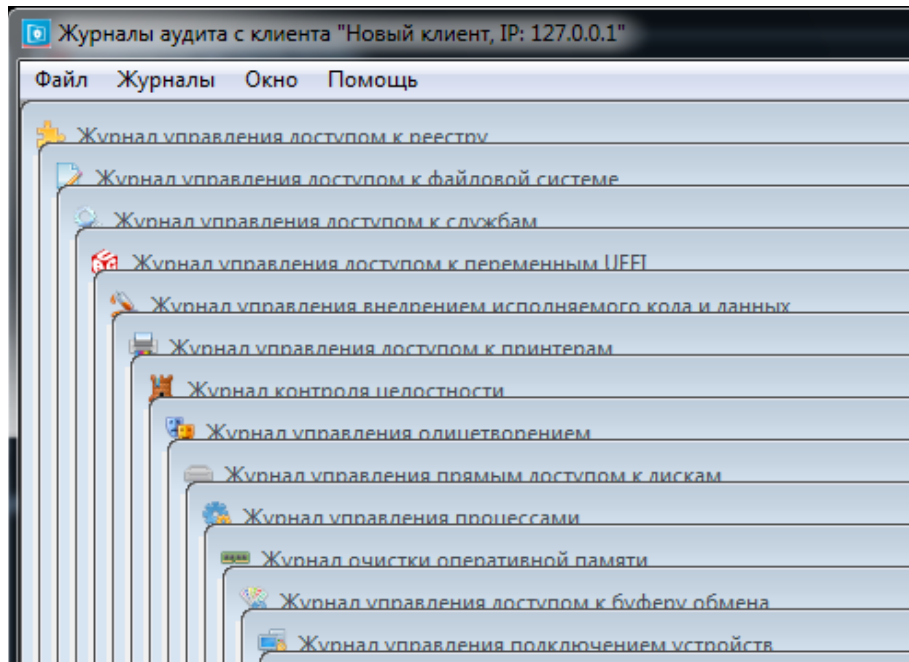
COM, LPT,  
FIREWIRE, IEEE  
1284.4

Wi-Fi,  
Bluetooth, MTP,  
сетевые  
адаптеры,  
модемы, смарт-  
карты, ИК

принтеры,  
дисководы,  
ленточные,  
любые съемные  
носители и  
устройства Plug  
and Play

# Аудит событий безопасности

Сервер аудита –  
осуществляет  
регистрацию событий  
в реальном времени



## СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

### СЕРТИФИКАТ СООТВЕТСТВИЯ № 4468

Внесен в государственный реестр системы сертификации  
средств защиты информации по требованиям безопасности информации  
18 октября 2021 г.

Выдан: 18 октября 2021 г.  
Действителен до: 18 октября 2026 г.

Настоящий сертификат удостоверяет, что изделие «VIPNet SafePoint», разработанное и производимое АО «ИфоТеКс», является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, 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 средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средства контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности и заданию по безопасности ФРКЕ.00240-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00240-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 15.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 05.10.2021, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИфоТеКс»  
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29  
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



*В.Лютиков*

В.Лютиков

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

# Сертифицировано

- 5 класс защищенности СВТ
- 4 класс защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 класс ТДБ



The background of the slide is a server room with rows of server racks. Overlaid on this are various digital graphics: a large globe, several bar charts, and two circular progress indicators. The left indicator shows '72%' and the right one shows '82%'. The overall color scheme is light blue and white, with a subtle grid pattern.

# VIPNet SafePoint 1.5

# VIPNet SafePoint 1.5



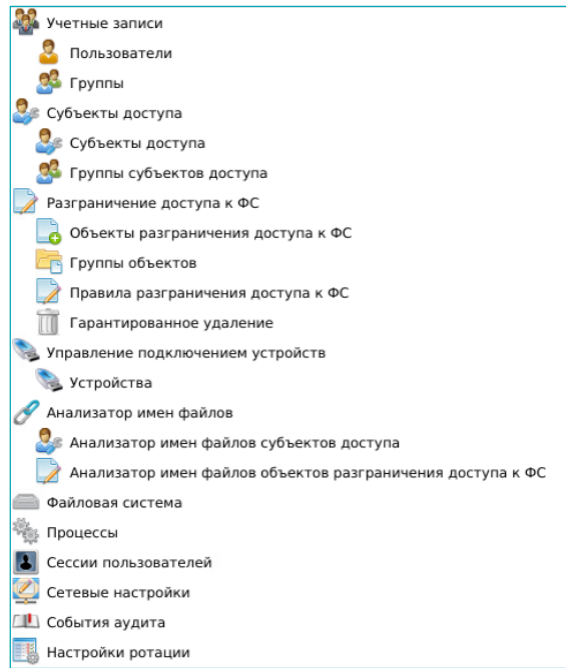
Главное - Разработан Клиент Linux с функциональностью необходимой для соответствия требованиям СВТ5 и СКН4.

Поддерживаемые ОС:

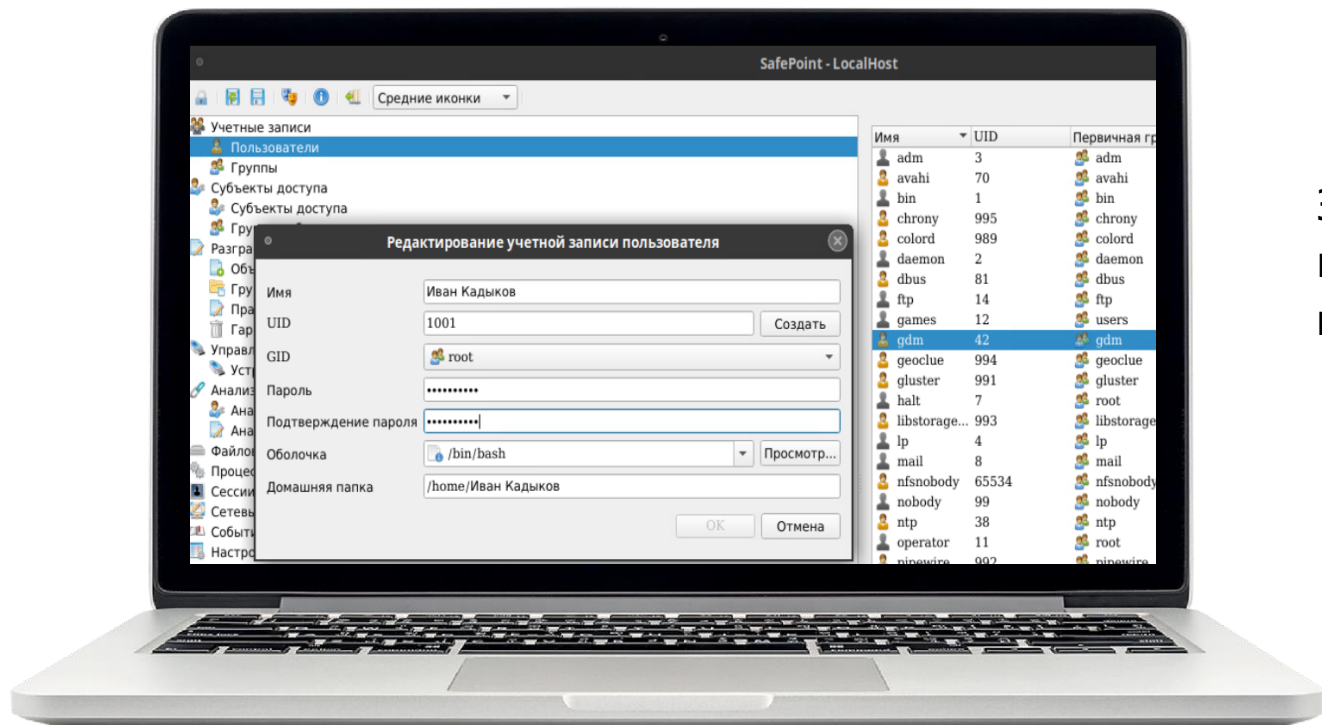
- Альт Рабочая станция 10.0, ядро Linux (std-def) 5.10.82
- РЕД ОС 7.3.1 МУРОМ x86\_64, ядро Linux 5.15.10 (Рабочая станция)
- Debian 11 (64-разрядная), ядро 5.10.0-10-amd64
- Astra Linux Special Edition, РУСБ.10015-01 (Astra Linux Special Edition 1.7 «Воронеж» и «Орёл») – без режима замкнутой программной среды

# Функциональность Linux агента

- Идентификация и аутентификация пользователей (без токенов)
- управление учетными записями
- дискреционное разграничение доступа
- управление подключением устройств
- гарантированное удаление файлов
- очистка дисковых томов
- самотестирование и контроль целостности
- аудит событий безопасности



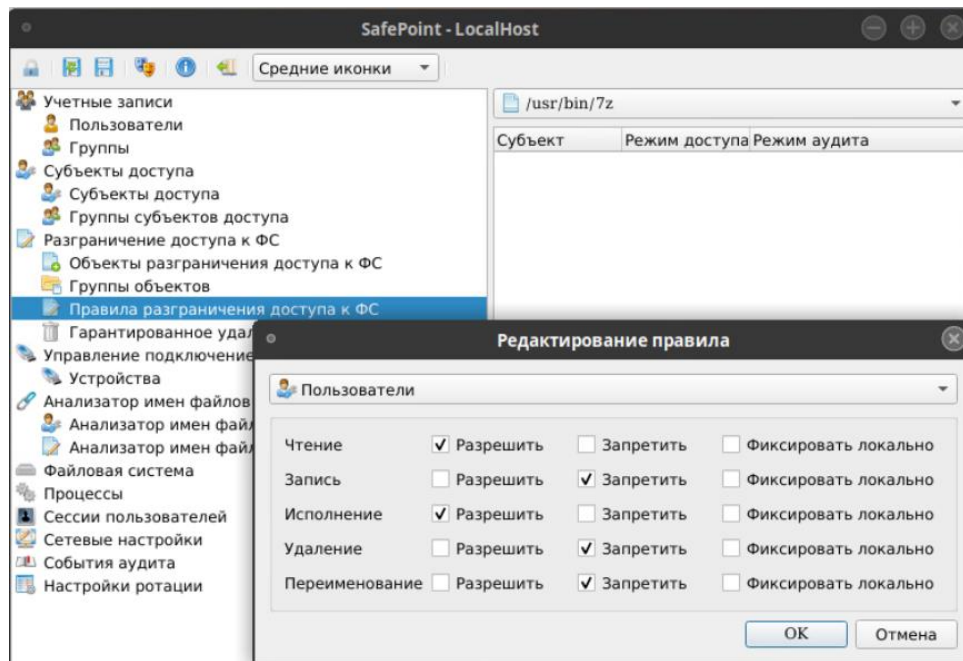
# Идентичность интерфейсов



Заведение  
и редактирование  
пользователей

# Идентичность интерфейсов

Правила разграничения доступа к файловой системе

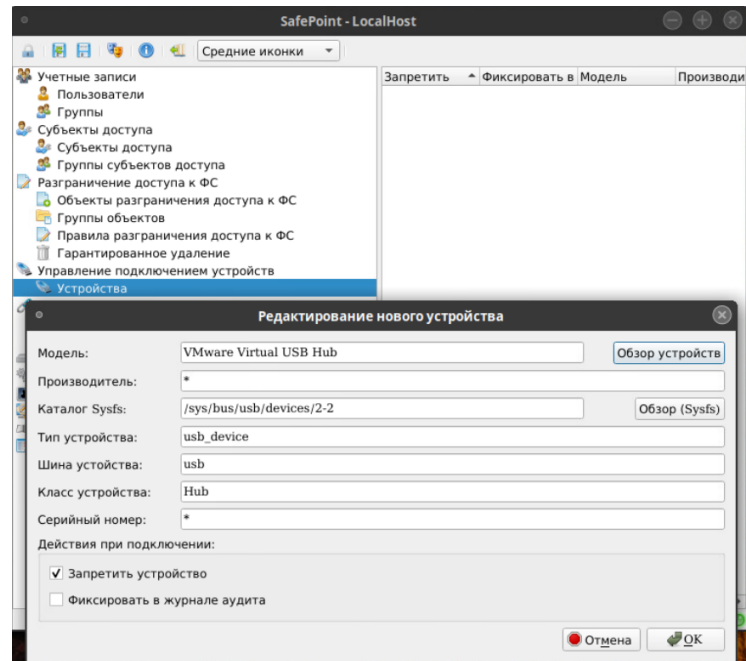


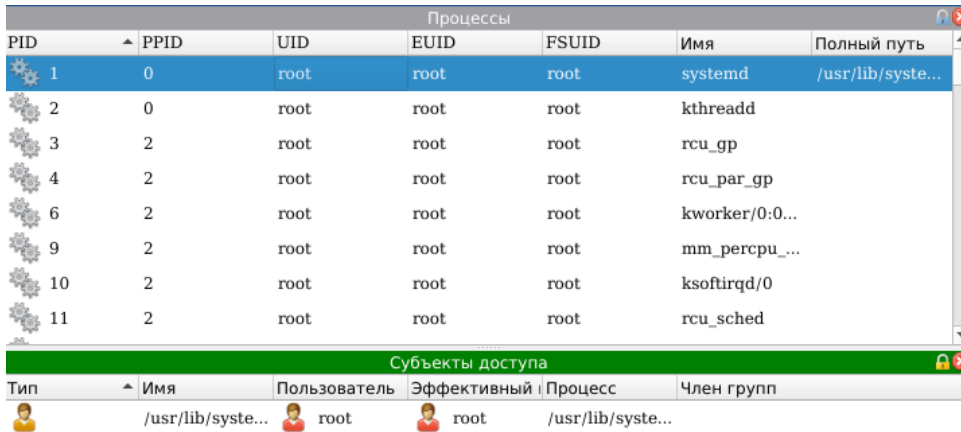


# Управление подключением устройств

Создание политик для подключаемых устройств:

- Если устройство хотя бы 1 раз было подключено, то вы его найдёте по кнопке «обзор устройств»
- После выбора - все поля заполнятся автоматически





The screenshot shows a terminal window with two panels. The top panel, titled 'Процессы', displays a list of system processes. The bottom panel, titled 'Субъекты доступа', shows the access subjects for the selected process (systemd).

PID	PPID	UID	EUID	FSUID	Имя	Полный путь
1	0	root	root	root	systemd	/usr/lib/systemd/systemd
2	0	root	root	root	kthreadd	
3	2	root	root	root	rcu_gp	
4	2	root	root	root	rcu_par_gp	
6	2	root	root	root	kworker/0:0...	
9	2	root	root	root	mm_percpu_...	
10	2	root	root	root	ksoftirqd/0	
11	2	root	root	root	rcu_sched	

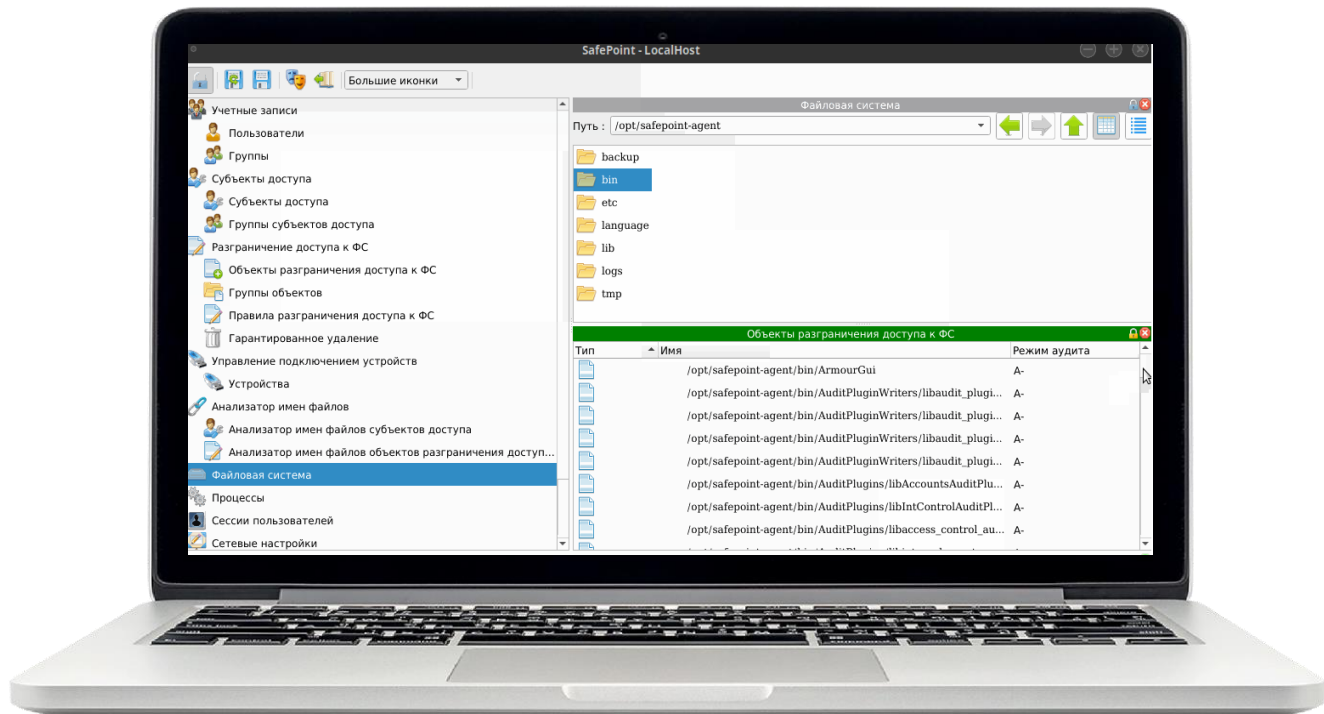
Тип	Имя	Пользователь	Эффективный	Процесс	Член групп
	/usr/lib/systemd/systemd	root	root	/usr/lib/systemd/systemd	

## Повышение удобства работы

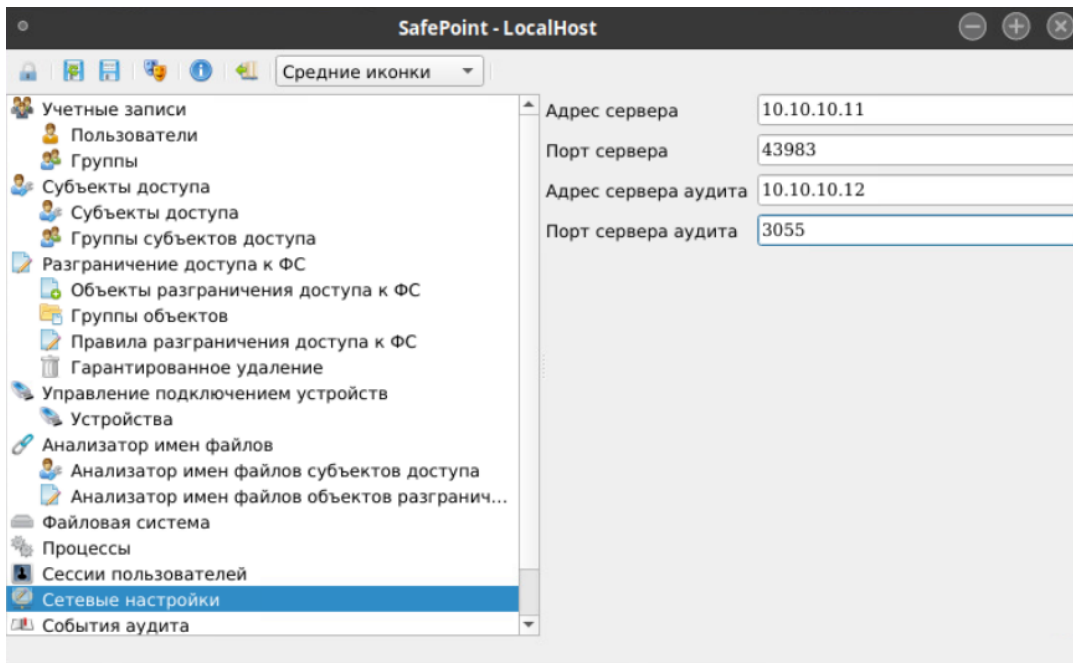
Для упрощения создания правил разграничения доступа в локальной консоли управления Клиента Linux вы можете закреплять одну или несколько вкладок и перетаскивать учетные записи, процессы, субъекты и объекты доступа между ними.

# Повышение удобства

Добавление  
объектов  
разграничения  
доступа  
к файловой  
системе

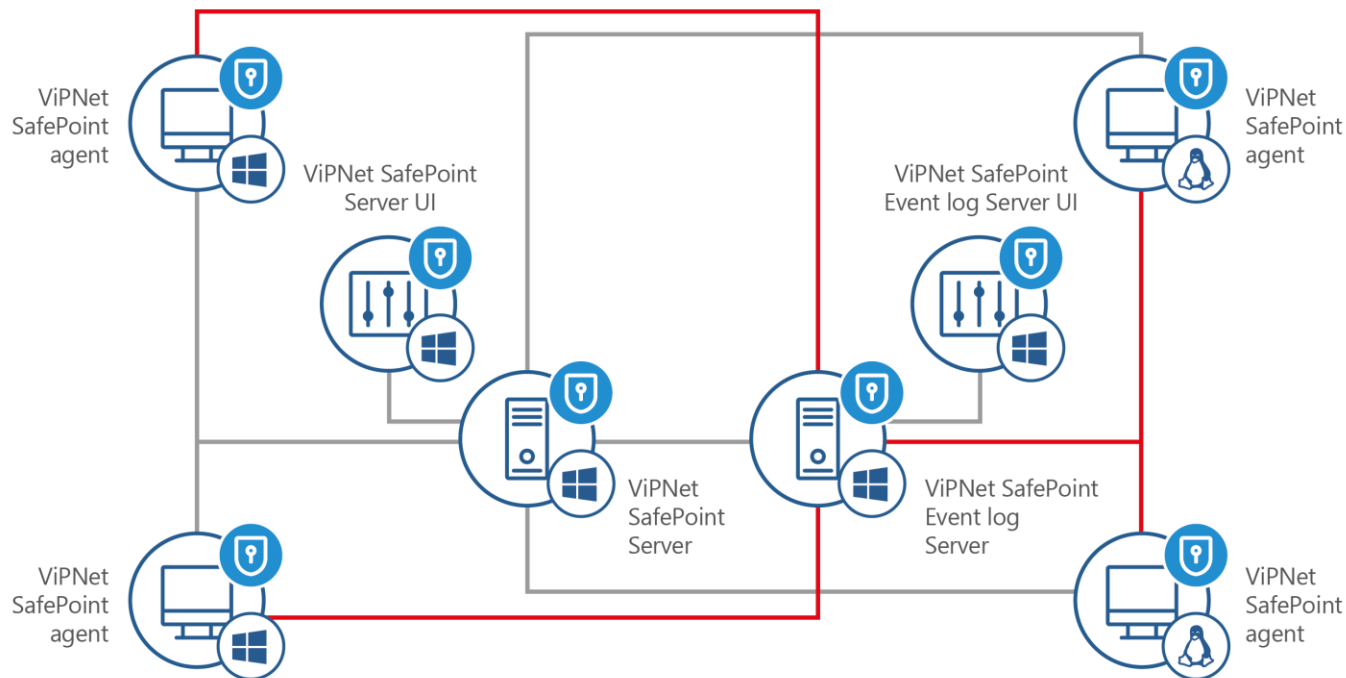


# Внедрение в имеющуюся инфраструктуру



Подключение к существующему серверу безопасности и серверу аудита не займёт много времени

# Архитектура



# Лицензирование

## Ничего не меняется

Комплект ViPNet SafePoint  
состоит из:

- Сервера Win
- Агента Lin (deb и rpm пакеты)
- Агента Win

Лицензия:

- «сетевая» на возможность подключения N-количества агентов
- «Автономная» для работы агента без сервера





# Перспективы развития





Стараемся работать над SafePoint версия 1.6:

- Расширение шаблонов политик безопасности по требованиям приказов 17,21,31,239
- Реализация мандатных меток на устройства (перемещение файлов с метками)
- Динамический контроль целостности
- Мандатная модель в линукс агенте
- SSO с SafeBoot в линукс агенте
- Поддержка токенов для идентификации/аутентификации для линукс агентов
- Поддержка новых ОС Linux



Спасибо за внимание!

**Иван Кадыков**

Руководитель направления

e-mail: [Ivan.Kadykov@infotecs.ru](mailto:Ivan.Kadykov@infotecs.ru)

---

Подписывайтесь на наши соцсети

---



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)