

VIPNet SafePoint 1.2

новая сертифицированная версия

Кадыков Иван
Руководитель направления


infotecs



Вместо введения

Продолжительное время говорили...



- Количество атак растёт
- Хищение и шифрование данных
- Регулярно происходят утечки данных
- Необходимо защищать свою ИТ-инфраструктуру
- Важно выстраивать доверие к пользователю и среде в которой он работает

Главная парадигма – Доверие!

Доверенная платформа

- Неизменность BIOS
- Неизменность Аппаратных составляющих
- Исключение возможности попадания или работы зловредного обеспечения в UEFI BIOS

Доверенный пользователь

- Легитимный пользователь
- Пользователь обладающий необходимым набором прав доступа
- Неспособный навредить системе (по неосторожности или целенаправленно)

Доверенная операционная система

- Доверенная загрузка ОС
- Замкнутая программная среда
- Мониторинг и противодействие подозрительной активности на хосте
- Защита и предотвращение сетевых атак
- Защита от внедрения и выполнения вредоносных программ и кода



«Российский Endpoint»

Средство защиты
от несанкционированного
доступа

Защита от инсайдеров

Инсайдеров можно разделить на следующие типы:

- Инсайдеры, готовые использовать любую информацию в личных целях для получения выгоды
- «Шпионы» – промышленный шпионаж
- «Обиженные» сотрудники
- Безответственные сотрудники (с низкой цифровой грамотностью)



Что может заменить СЗИ от НСД

Application Control – контроль приложений

Device Control – контроль устройств

Identity and Access Management – управление доступом

Privileged users management (PUM) – управление привилегированными пользователями

Data Integrity Control – Контроль целостности данных

The logo for 'infotecs' is located in the top right corner. It consists of the word 'infotecs' in a dark blue, lowercase sans-serif font. A red curved line is positioned above the 'i' and 'f'.

**У нас
есть, что
предложить**

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

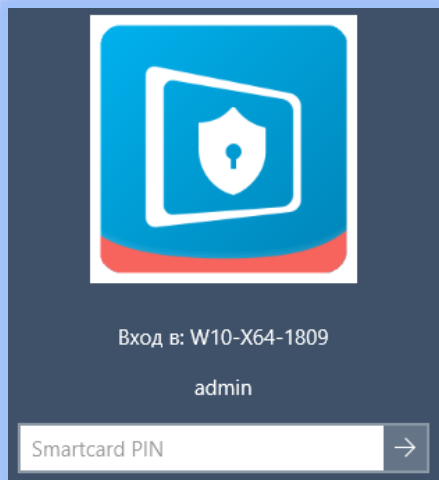
Используем комбинации:

- Логин и пароль
- Логин и идентификатор



Поддержка USB-токенов и смарт-карт

- JaCarta PKI
- JaCarta PKI/ГОСТ
- JaCarta 2
PKI/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

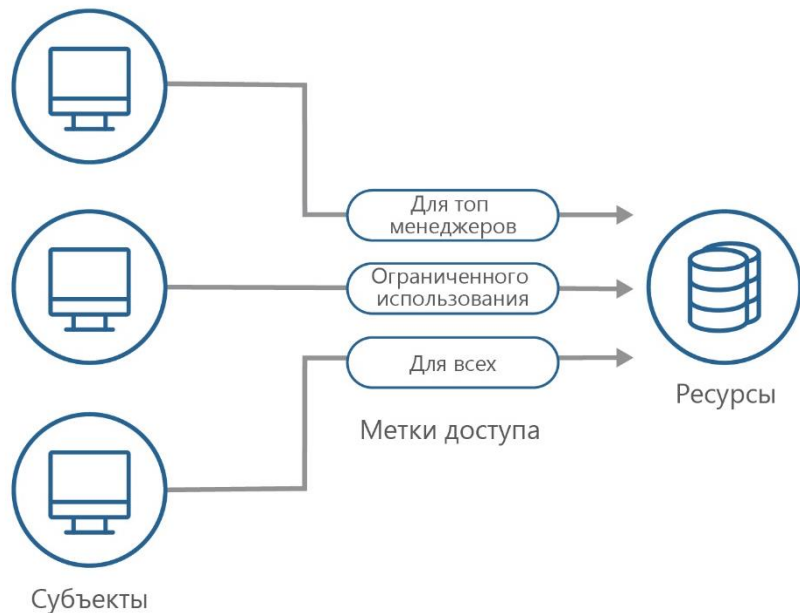
Разграничение доступа

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)

Отличительные черты ЗПС в ViPNet SafePoint

Защита от модификации
запускаемых модулей

Контроль запуска скриптов
Active Scripts

Контроль запуска задач



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

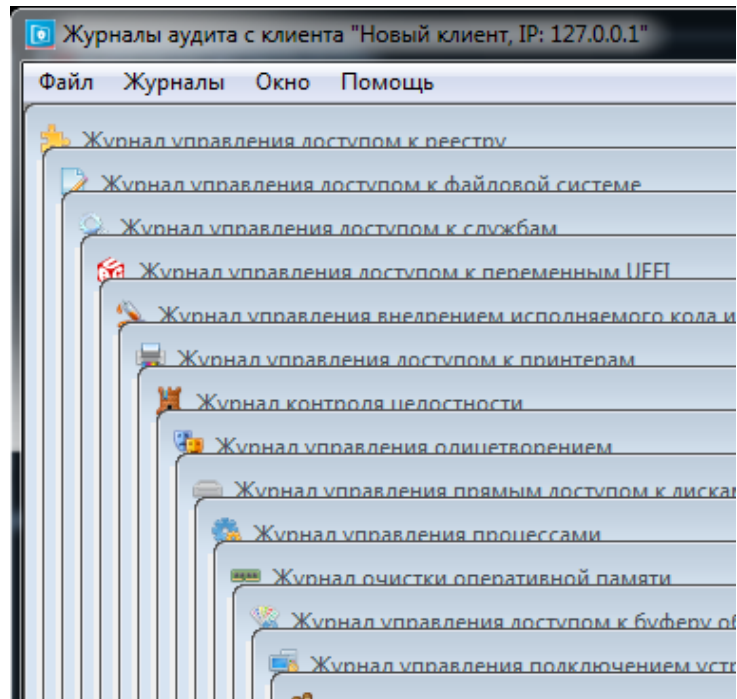
принтеры,
дисководы,
ленточные,
любые съемные
носители и
устройства Plug
and Play

Контроль устройств

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

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 «ИнфоТекС», 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 «НИИФ» (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 «ИнфоТекС»
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

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

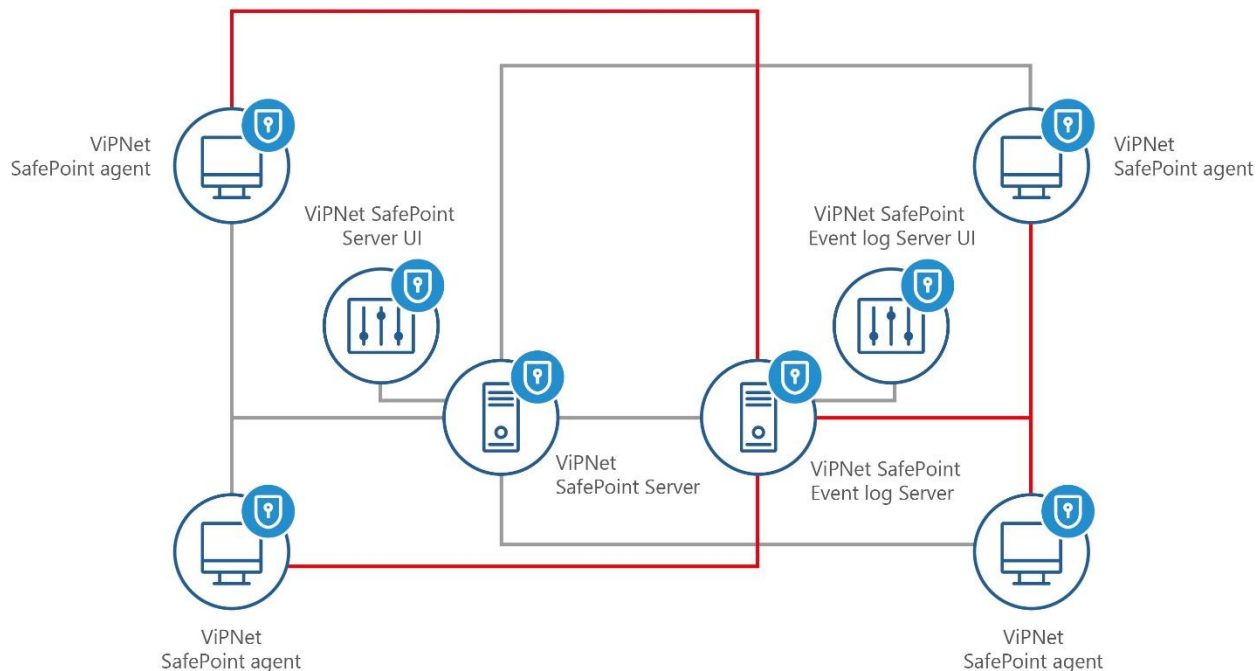
Сертифицировано

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

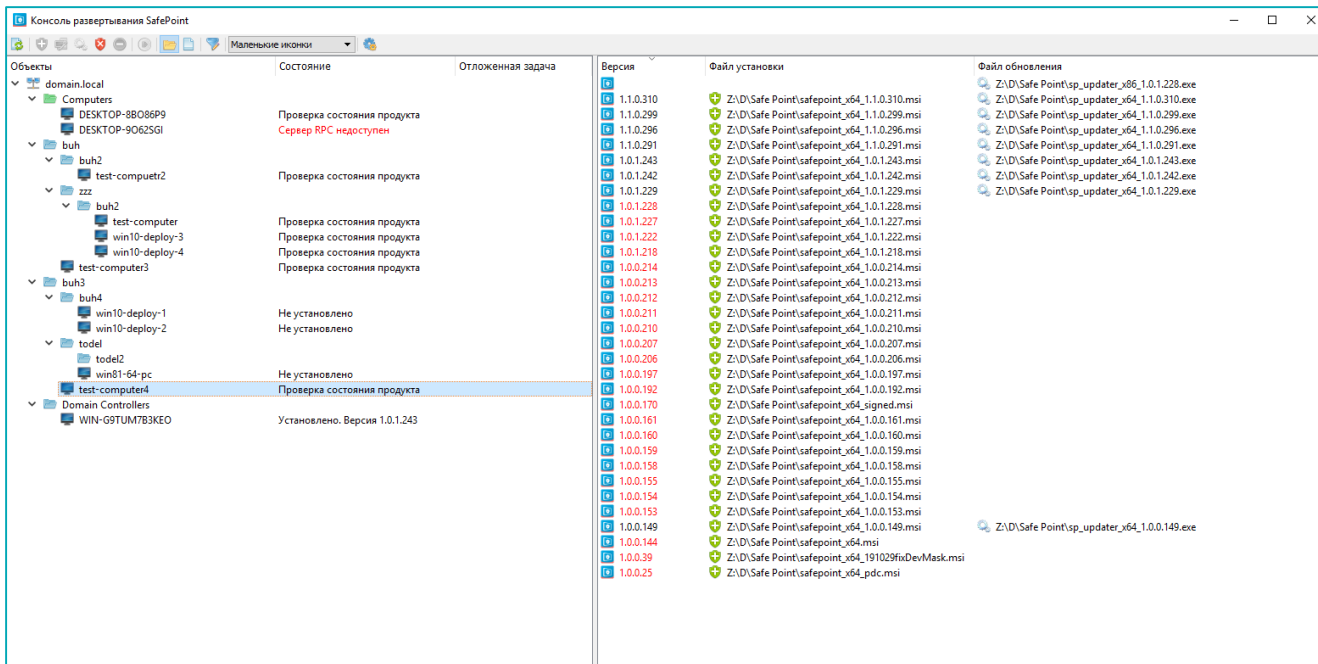
The logo for infotecs, featuring a red curved line above the word "infotecs" in a dark blue, lowercase sans-serif font.

VIPNet SafePoint 1.2

Одновременная работа нескольких администраторов с сервером



Централизованная установка и обновление продукта



Консоль развертывания SafePoint

Объекты	Состояние	Отложенная задача	Версия	Файл установки	Файл обновления
domain.local					
Computers					
DESKTOP-8B086P9	Проверка состояния продукта		1.1.0.310	Z:\D:\Safe Point\safepoint_x64_1.1.0.310.msi	Z:\D:\Safe Point\sp_updater_x86_1.0.1.228.exe
DESKTOP-90625G1	Сервер RPC недоступен		1.1.0.299	Z:\D:\Safe Point\safepoint_x64_1.1.0.299.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.299.exe
buh			1.1.0.296	Z:\D:\Safe Point\safepoint_x64_1.1.0.296.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.296.exe
buh2			1.1.0.291	Z:\D:\Safe Point\safepoint_x64_1.1.0.291.msi	Z:\D:\Safe Point\sp_updater_x64_1.1.0.291.exe
test-compuert2	Проверка состояния продукта		1.0.1.243	Z:\D:\Safe Point\safepoint_x64_1.0.1.243.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.243.exe
zzz			1.0.1.242	Z:\D:\Safe Point\safepoint_x64_1.0.1.242.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.242.exe
buh2			1.0.1.229	Z:\D:\Safe Point\safepoint_x64_1.0.1.229.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.1.229.exe
test-computer	Проверка состояния продукта		1.0.1.228	Z:\D:\Safe Point\safepoint_x64_1.0.1.228.msi	
win10-deploy-3	Проверка состояния продукта		1.0.1.227	Z:\D:\Safe Point\safepoint_x64_1.0.1.227.msi	
win10-deploy-4	Проверка состояния продукта		1.0.1.222	Z:\D:\Safe Point\safepoint_x64_1.0.1.222.msi	
test-computer3	Проверка состояния продукта		1.0.1.218	Z:\D:\Safe Point\safepoint_x64_1.0.1.218.msi	
buh3			1.0.0.214	Z:\D:\Safe Point\safepoint_x64_1.0.0.214.msi	
buh4			1.0.0.213	Z:\D:\Safe Point\safepoint_x64_1.0.0.213.msi	
win10-deploy-1	Не установлено		1.0.0.212	Z:\D:\Safe Point\safepoint_x64_1.0.0.212.msi	
win10-deploy-2	Не установлено		1.0.0.211	Z:\D:\Safe Point\safepoint_x64_1.0.0.211.msi	
todel			1.0.0.210	Z:\D:\Safe Point\safepoint_x64_1.0.0.210.msi	
todel2			1.0.0.207	Z:\D:\Safe Point\safepoint_x64_1.0.0.207.msi	
win81-64-pc	Не установлено		1.0.0.206	Z:\D:\Safe Point\safepoint_x64_1.0.0.206.msi	
test-computer4	Проверка состояния продукта		1.0.0.197	Z:\D:\Safe Point\safepoint_x64_1.0.0.197.msi	
Domain Controllers			1.0.0.192	Z:\D:\Safe Point\safepoint_x64_1.0.0.192.msi	
WIN-GSTUM7B3KE0	Установлено. Версия 1.0.1.243		1.0.0.170	Z:\D:\Safe Point\safepoint_x64_signed.msi	
			1.0.0.161	Z:\D:\Safe Point\safepoint_x64_1.0.0.161.msi	
			1.0.0.160	Z:\D:\Safe Point\safepoint_x64_1.0.0.160.msi	
			1.0.0.159	Z:\D:\Safe Point\safepoint_x64_1.0.0.159.msi	
			1.0.0.158	Z:\D:\Safe Point\safepoint_x64_1.0.0.158.msi	
			1.0.0.155	Z:\D:\Safe Point\safepoint_x64_1.0.0.155.msi	
			1.0.0.154	Z:\D:\Safe Point\safepoint_x64_1.0.0.154.msi	
			1.0.0.153	Z:\D:\Safe Point\safepoint_x64_1.0.0.153.msi	
			1.0.0.149	Z:\D:\Safe Point\safepoint_x64_1.0.0.149.msi	Z:\D:\Safe Point\sp_updater_x64_1.0.0.149.exe
			1.0.0.144	Z:\D:\Safe Point\safepoint_x64.msi	
			1.0.0.39	Z:\D:\Safe Point\safepoint_x64_191029fixDevMask.msi	
			1.0.0.25	Z:\D:\Safe Point\safepoint_x64_pdc.msi	

Ограничение действий администраторов

- Реализация настраиваемых ограничений в действиях администраторов – в части управления пользователями в Active Directory
- Делегирование административных полномочий (полных прав/части прав)

Редактирование роли администратора

Имя роли:

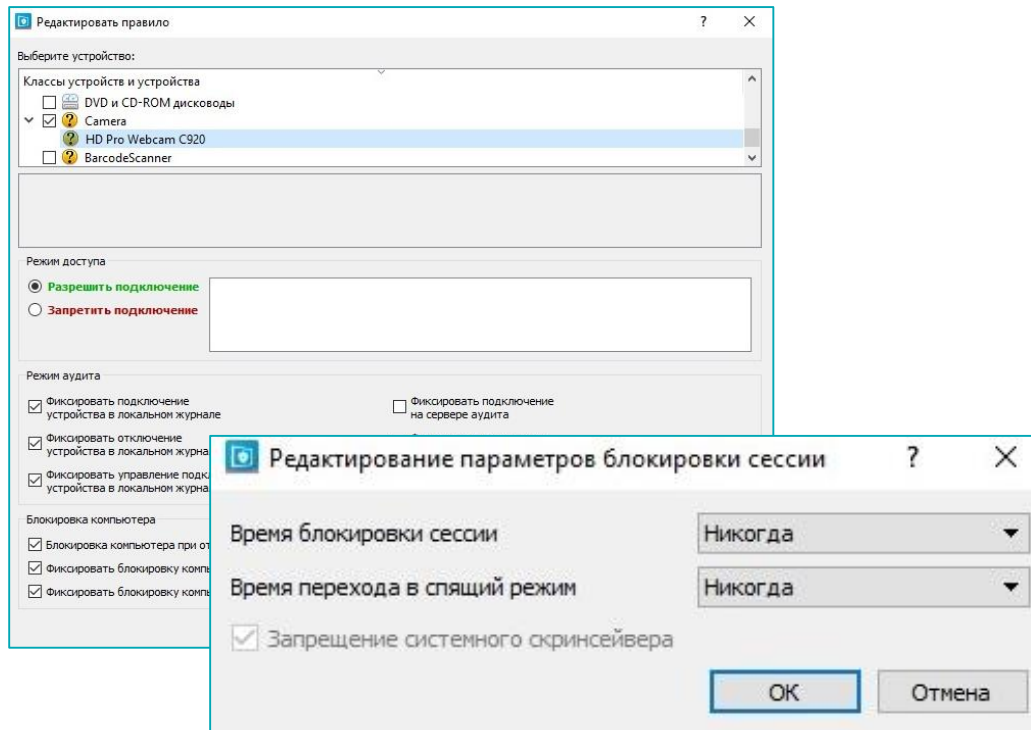
Дополнительная информация:
Администраторы SafePoint
Имеют все привилегии для управления настройками SafePoint, за исключением возможности управления списком администраторов.

Разрешенные действия на клиенте	Разрешенные действия на сервере
<input checked="" type="checkbox"/> Управление списком клиентов сервера	<input checked="" type="checkbox"/> Управление службой сервера
<input checked="" type="checkbox"/> Разрыв соединения	<input checked="" type="checkbox"/> Просмотр администраторов <input type="checkbox"/> Управление администраторами
<input checked="" type="checkbox"/> Просмотр аудита клиента	<input type="checkbox"/> Изменение паролей администраторов
<input checked="" type="checkbox"/> Просмотр ФС клиента	<input type="checkbox"/> Управление ролями администраторов
<input checked="" type="checkbox"/> Просмотр реестра клиента	<input checked="" type="checkbox"/> Просмотр аудита сервера <input checked="" type="checkbox"/> Очистка аудита сервера
<input checked="" type="checkbox"/> Просмотр работающих процессов	<input checked="" type="checkbox"/> Просмотр ФС сервера <input checked="" type="checkbox"/> Управление ФС сервера
<input checked="" type="checkbox"/> Просмотр настроек SafePoint	<input checked="" type="checkbox"/> Управление лицензией
<input checked="" type="checkbox"/> Общее управление настройками SafePoint	
<input checked="" type="checkbox"/> Обновление клиента	
<input checked="" type="checkbox"/> Управление службой клиента	
<input checked="" type="checkbox"/> Управление ФС клиента	
<input checked="" type="checkbox"/> Управление реестром клиента	
<input checked="" type="checkbox"/> Управление работающими процессами	
<input checked="" type="checkbox"/> Управление настройками SafePoint	
<input checked="" type="checkbox"/> Автоматическое управление настройками SafePoint	

OK Отмена

Дополнительные возможности для блокировки компьютера

- Возможность блокировки компьютера при подключении или отключении заданных устройств
- Возможность блокировки сессии пользователя по периоду неактивности и событию



SSO (единый вход) для SafeBoot и SafePoint

В интерфейс SafePoint при добавлении/изменении пользователя добавлен дополнительный флаг:

- «Разрешить вход SSO (режим единого входа)»

Флаг является индивидуальным для каждого пользователя.

Поддерживаемые версии

- ViPNet SafeBoot 2.1
- ViPNet SafeBoot 3.0

Редактирование данных пользователя

Пользователь: DESKTOP-SECQVOA\User1

Доверять паролю Windows

Пароль SafePoint:

Подтвердите пароль:

Пароль Windows:

Подтвердите пароль Windows:

Разрешить пользователю осуществлять вход с помощью:

Ввода имени и пароля

Электронного ключа ruToken

Электронного ключа Aladdin JaCarta

Записать данные на смарт-карту/эл.ключ

Разрешить вход при работе ОС в безопасном режиме

Разрешить вход SSO (режим единого входа)

OK Отмена

Контроль межпроцессного взаимодействия

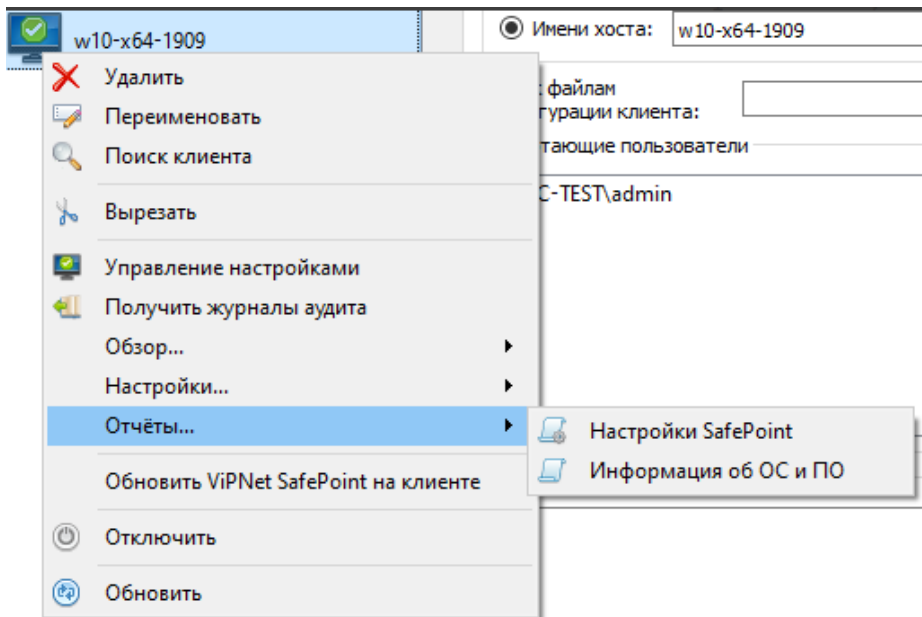
В механизм «Управление доступом к буфера обмена» SafePoint добавлены:

- Контроль передачи данных через OLE (Object Linking & Embedding)
- Контроль передачи данным через Drag and Drop (Перетаскивание объектов)

Просмотрщик журналов аудита - [Журнал управления доступом к буферу обмена]

№	Время	Процесс, осуществляющий доступ	Пользователь, осуществл	Процесс, поместивший информацию ранее	Пользователь, поместивший	Операция	Описание
3	Пт 10/07/2020 1...	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	Поместил информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
4	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
5	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
6	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
7	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
8	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Поместил информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
9	Пт 10/07/2020 1...	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Доступ запрещён
10	Пт 10/07/2020 1...	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	Поместил информацию типа 15 (через OLE или Drag'n'Drop)	Успешно
11	Пт 10/07/2020 1...	C:\Program Files\WinRAR\WinRAR.exe	DESKTOP-SECQVOA\xms	C:\WINDOWS\Explorer.EXE	DESKTOP-SECQVOA\xms	Взял информацию типа 15 (через OLE или Drag'n'Drop)	Доступ запрещён

Отчёты о настройках продукта и установленном ПО



Возможность построения отчётов о:

- Настройках продукта (включённой функциональности)
- Информация об Операционной системе и установленном программном обеспечении

Прочие улучшения

- Отправка событий на электронную почту в внешние SIEM-системы
- Поддержка работы в среде Citrix XenApp и XenDesktop
- Поддержка новых электронных ключей и смарт-карт - JaCarta ГОСТ, JaCarta-2 SE, JaCarta-2 ГОСТ и JaCarta-2 PRO/ГОСТ
- Автоматизация настройки перечня контролируемых модулей (ЗПС)



Пока только...

Microsoft Windows 8.1 (64-разрядная)

Microsoft Windows 10 (64-разрядная)
версии 1803, 1809, 2004, 20H2, 21H1

Microsoft Windows 11 (64-разрядная)

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2016 версия 1607

Microsoft Windows Server 2019 (Standard)
версии 1809, 1909





ViPNet SafePoint 1.5 с поддержкой:

- Альт Рабочая станция 10.0
- РЕД ОС 7.3.1 МУРОМ(Рабочая станция)
- Debian 11 (64-разрядная)
- Astra Linux Special Edition 1.7



Спасибо за внимание!

Иван Кадыков

Руководитель направления

e-mail: Ivan.Kadykov@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363