ViPNet SafePoint – эффективная система защиты рабочих станций. Обзор возможностей продукта

Кадыков Иван
Руководитель направления

СЗИ от НСД
в современном ИБ мире

Историческая справка

Ключевой документ для сертификации СЗИ от НСД (с 1992):

- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссия России, 1992 г.

- Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Гостехкомиссия России, 1992 г.

С 2014 года выпущен

- Профиль защиты средств контроля подключения съемных машинных носителей информации

СВТ 5 – это как?

Необходимые показатели защищённости по 5 классу

- Дискреционный принцип контроля доступа
- Очистка памяти
- Идентификация и аутентификация
- Регистрация
- Целостность КСЗ

Всплеск развития

Появление различных нормативных документов, приказов, законов

Приказы ФСТЭК:

- №17 по защите государственных информационных систем (ГИС);
- №21 по защите информационных систем персональных данных (ИСПДн);
- №31 по защите автоматизированных систем управления технологическим процессом (АСУ ТП);
- №239 по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ (КИИ)

Ключевые механизмы защиты современным языком

- Application Control
- Device Control
- Identity and Access Management
- Privileged users management (PUM)
- Data Integrity Control

ViPNet SafePoint

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**

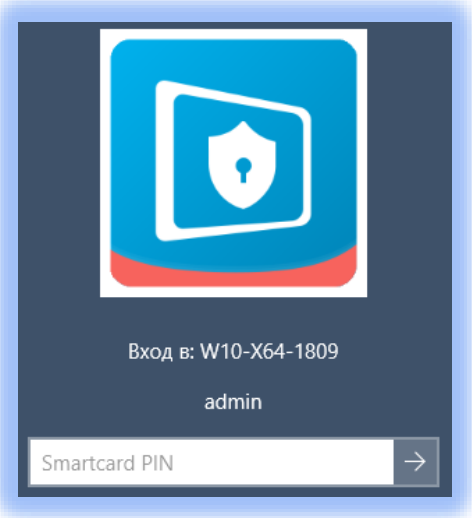
выполняется собственными механизмами

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

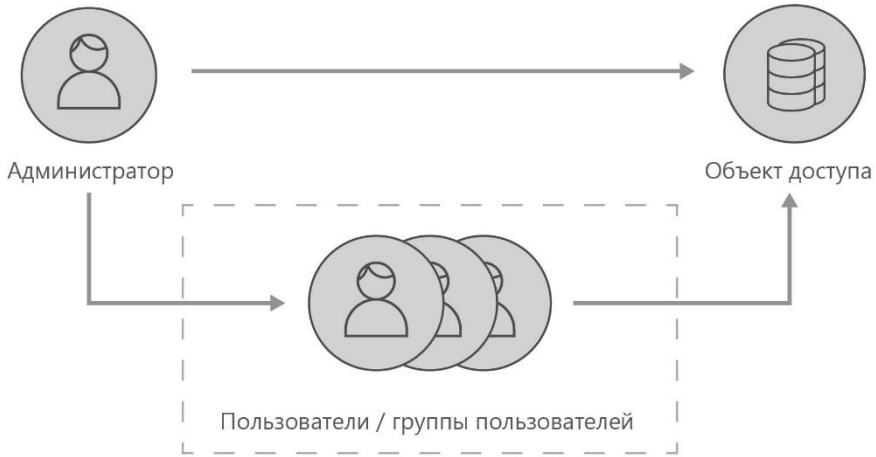
После прохождения идентификации и аутентификации, необходимо чтобы пользователь:

- 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

Разграничение доступа

Дискреционный контроль доступа к

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



Особенности реализации дискреционного доступа

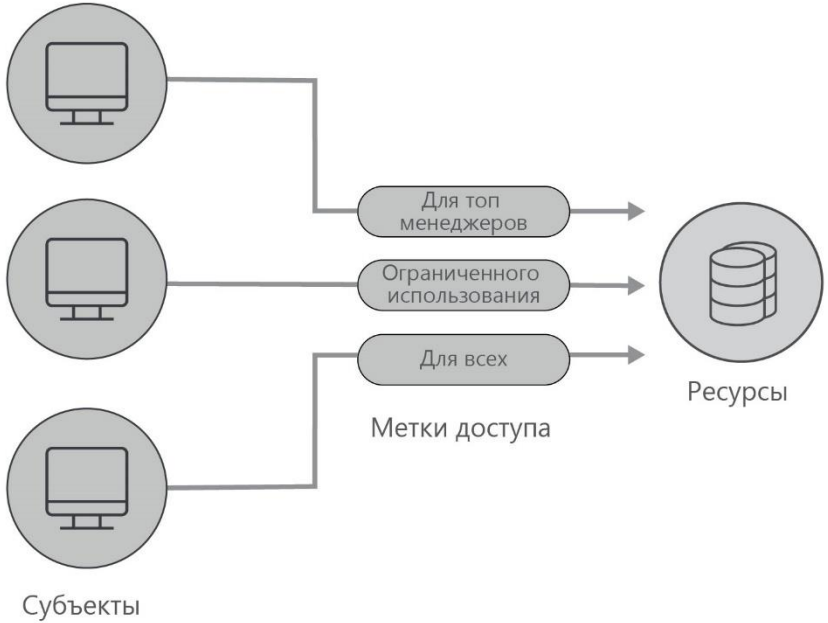
- В качестве субъекта доступа в разграничительной политике одновременно выступают три сущности:
  - исходный идентификатор пользователя SID
  - эффективный идентификатор пользователя (контекст безопасности (маркер-token) процесса при доступе)
  - «полнопутевое» имя процесса (имя исполняемого файла процесса)

- Такой подход позволяет задавать то, каким пользователем каким процессом разрешен доступ к какому ресурсу в рамках реализации той или иной роли

Последний актуальный кейс

- В Windows найдена уязвимость CVE-2021-41379
- Выявлена специалистами из Cisco Talos
- «Повышение привилегий в Microsoft Windows»
- 22.11.2021 выложен эксплоит на GitHub
- Один их вариантов эксплуатации – использование списка управления дискреционным доступом (DACL) в Microsoft Edge Elevation Service

ViPNet SafePoint использует свою дискреционную модель доступа, запрещает запуск того, что создано или изменено пользователем(элемент ЗПС).



Мандатный контроль доступа пользователей и процессов

Разграничительная политика на основе меток безопасности

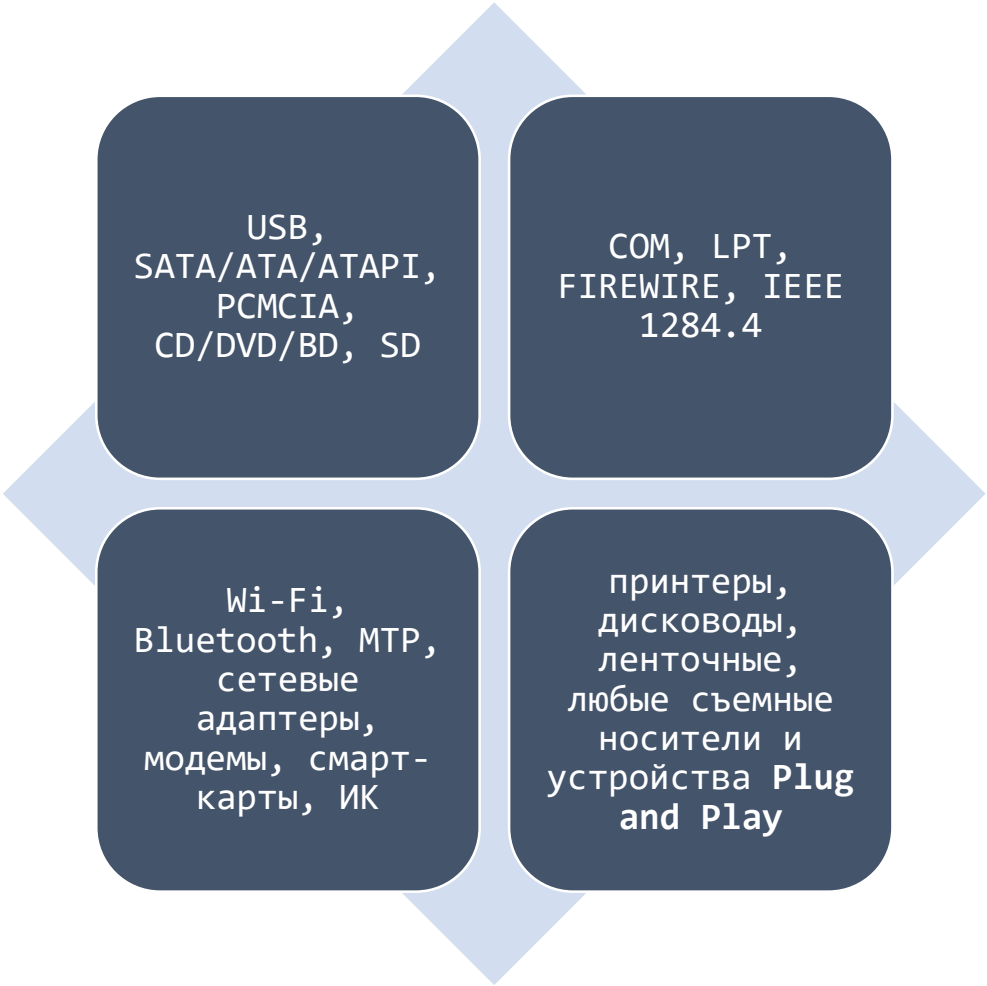
Замкнутая программная среда и контроль времени работы

Отличительные черты ЗПС в ViPNet SafePoint

Защита от модификации запускаемых модулей

Контроль запуска скриптов Active Scripts

Контроль запуска задач

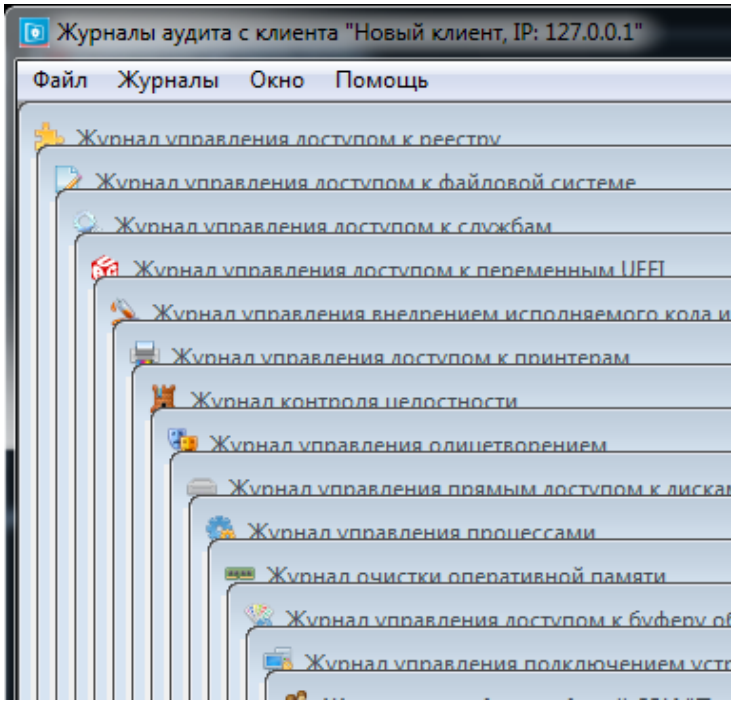


Контроль устройств

- 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 средств 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 задании 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 «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 информатизации) 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

Решаемые задачи

Защита от внедрения и выполнения вредоносных программ и кода

Защита от атак на повышение привилегий

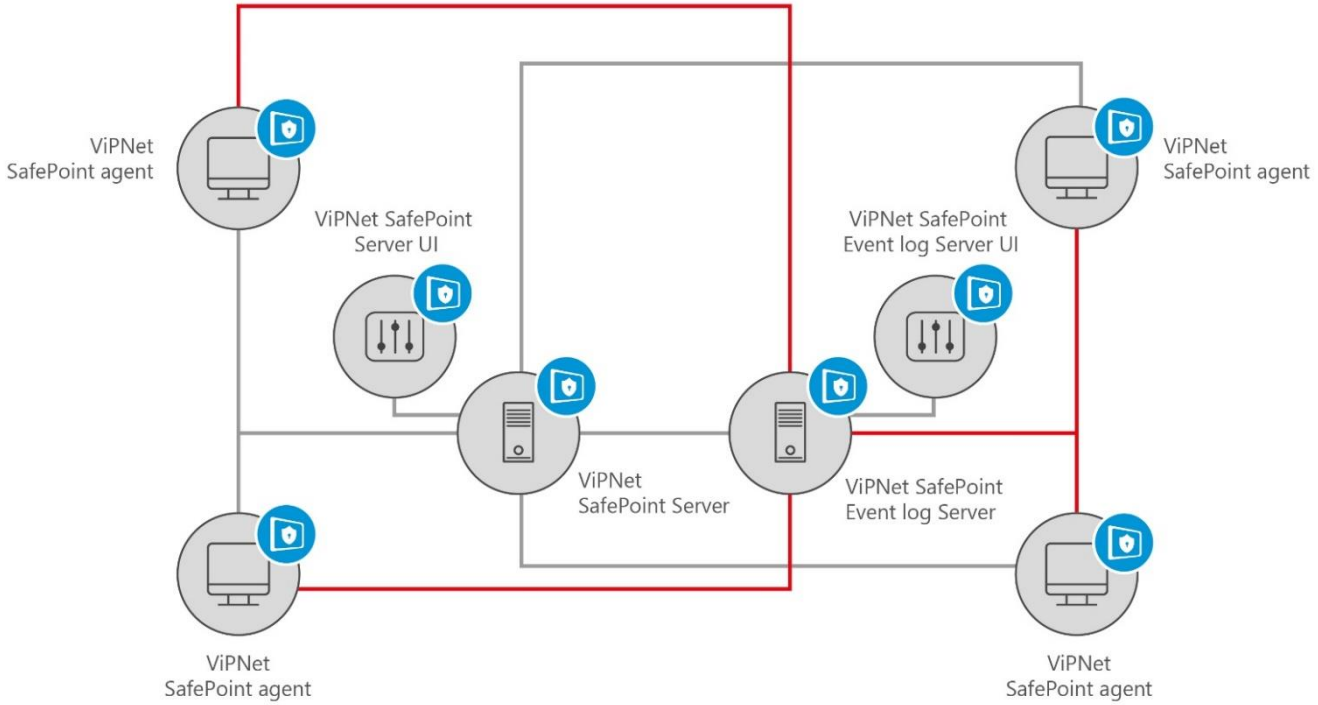
Защита данных от атак на уязвимости системного ПО

Защита от инсайдеров

Защита данных от атак на уязвимости прикладного ПО

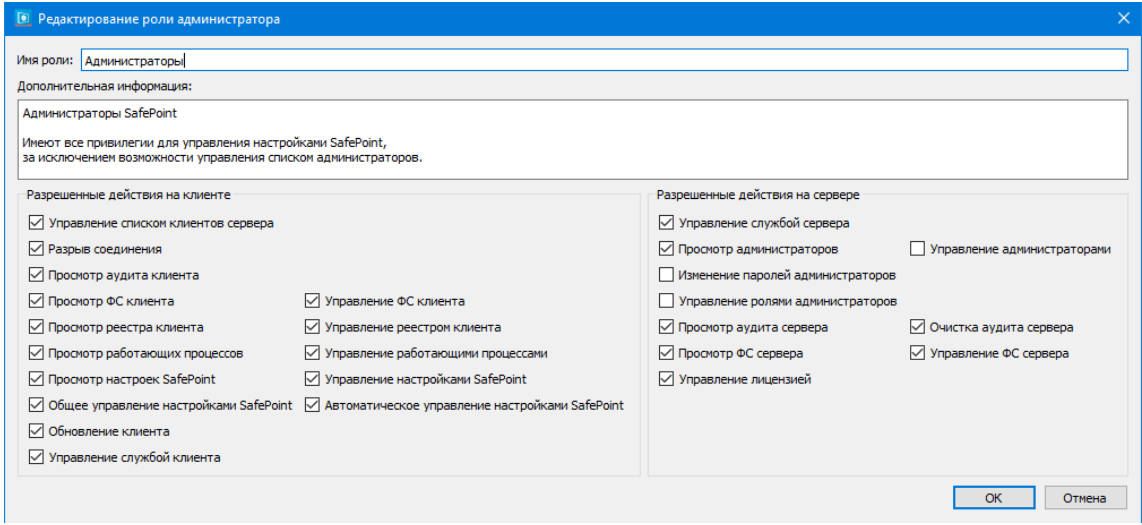
ViPNet SafePoint 1.2

Одновременная работа нескольких администраторов с сервером



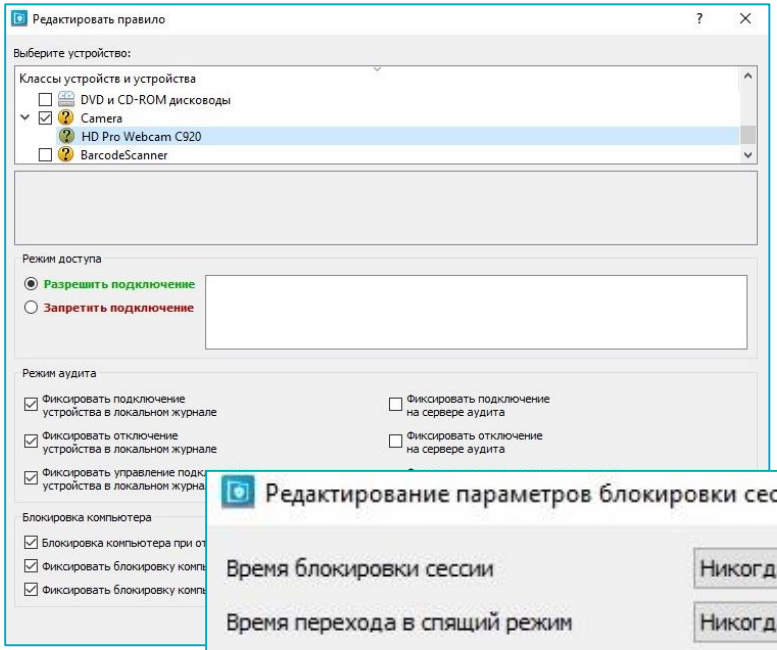
Ограничение действий администраторов

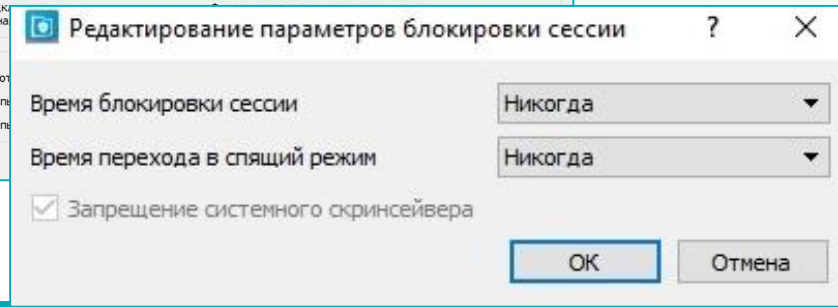
- Реализация настраиваемых ограничений в действиях администраторов – в части управления пользователями в Active Directory
- Делегирование административных полномочий (полных прав/части прав)



Дополнительные возможности для блокировки компьютера

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

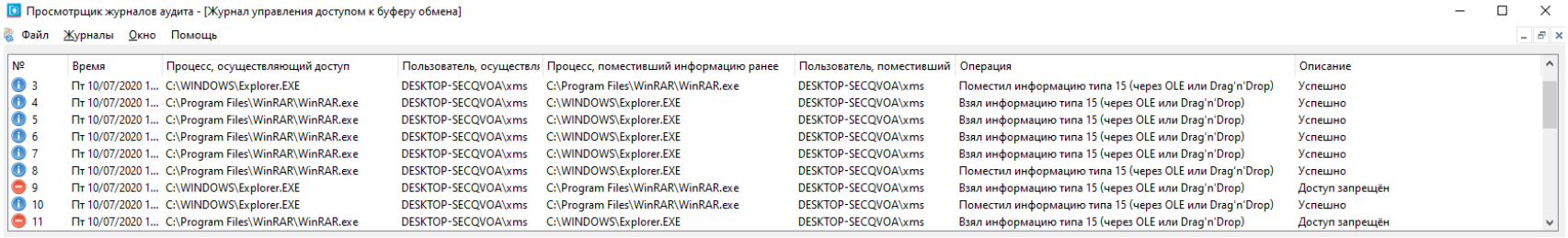




Контроль межпроцессного взаимодействия

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)



№	Время	Процесс, осуществляющий доступ	Пользователь, осуществля	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

SSO (единый вход) для SafeBoot и SafePoint

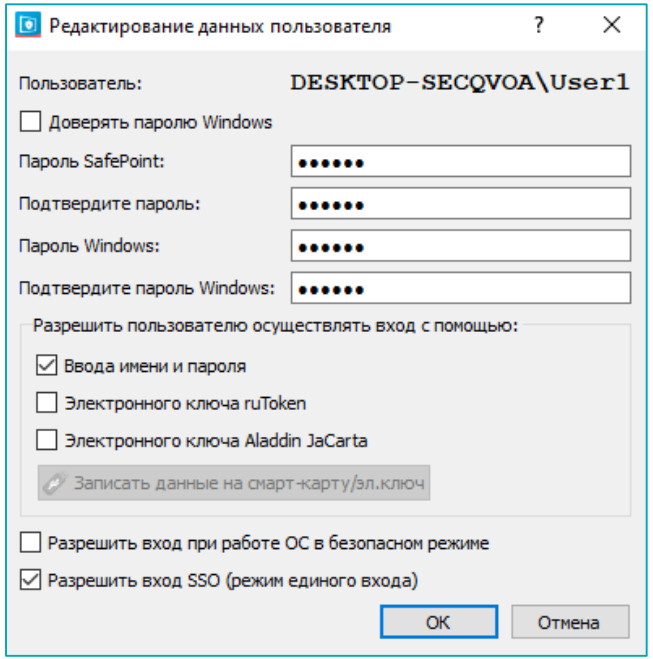
В интерфейс SafePoint при добавлении/изменении пользователя добавлен дополнительный флаг:

- «Разрешить вход SSO (режим единого входа)»

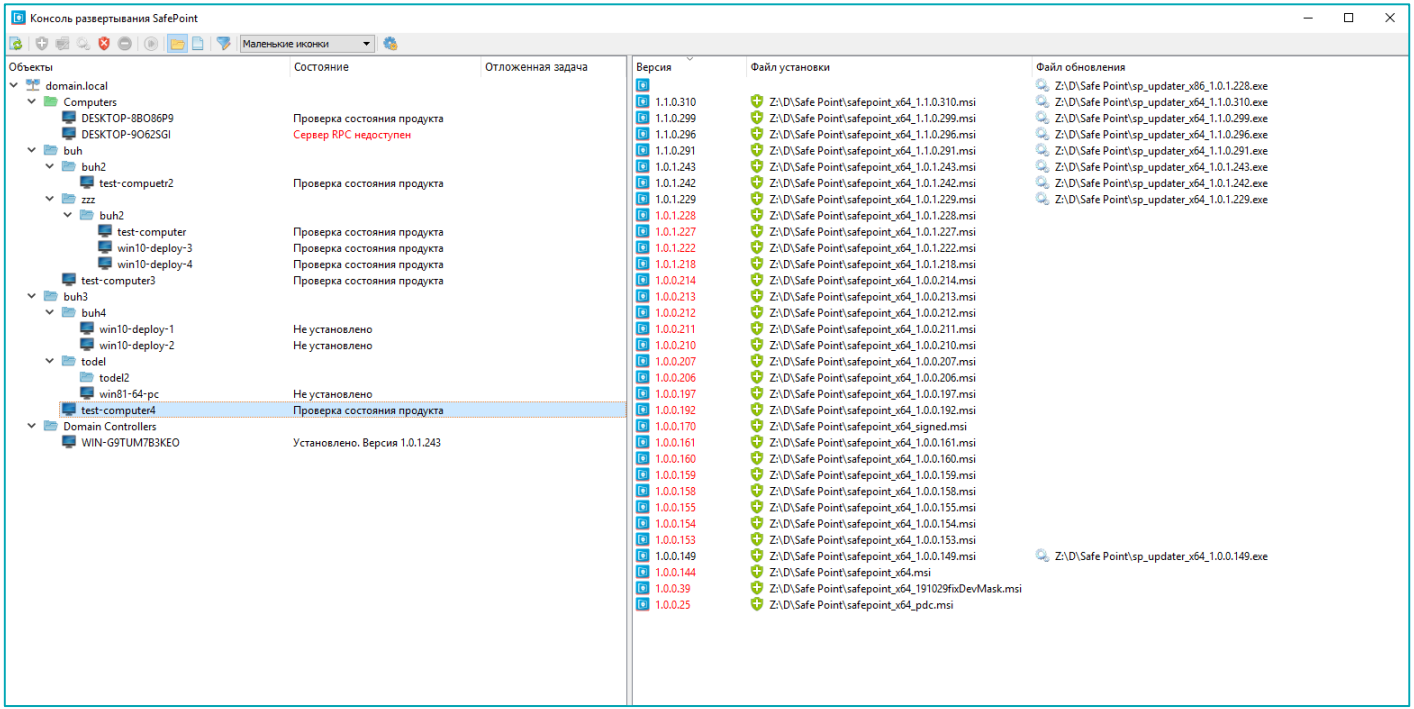
Флаг является индивидуальным для каждого пользователя.

Поддерживаемые версии

- ViPNet SafeBoot 2.1
- ViPNet SafeBoot 3.0



Централизованная установка и обновление продукта



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)
- Возможность построения отчётов о настройках продукта и установленном ПО

ViPNet SafePoint 1.2

Передан на контроль изменений.
Завершения контроля изменений
ожидаем в Q2 2022

Ответы на вопросы

Спасибо за внимание!

Иван Кадыков

Руководитель направления

e-mail: Ivan.Kadykov@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow