ViPNet SafePoint
Защита рабочих станций в современных реалиях

Кадыков Иван
Руководитель направления

Доверие

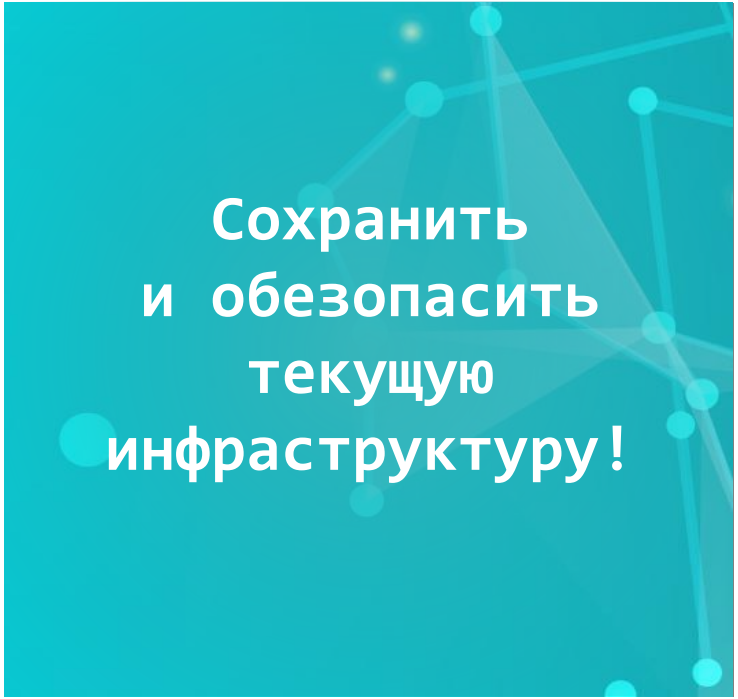
Доверие – это убежденность
в чьей-нибудь честности,
порядочности, веры в искренность
и добросовестность кого-нибудь.

Нарушены цепочки…

То, что недавно казалось надежным и внушало уверенность, перестало являться таковым

- Уходим
- Отключаем
- Останавливаем
- Отворачиваемся

Первоочередная задача



Для рабочих станций и серверов это:

- Операционные системы
- Общесистемное программное обеспечение
- Специальное программное обеспечение
- Данные

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)

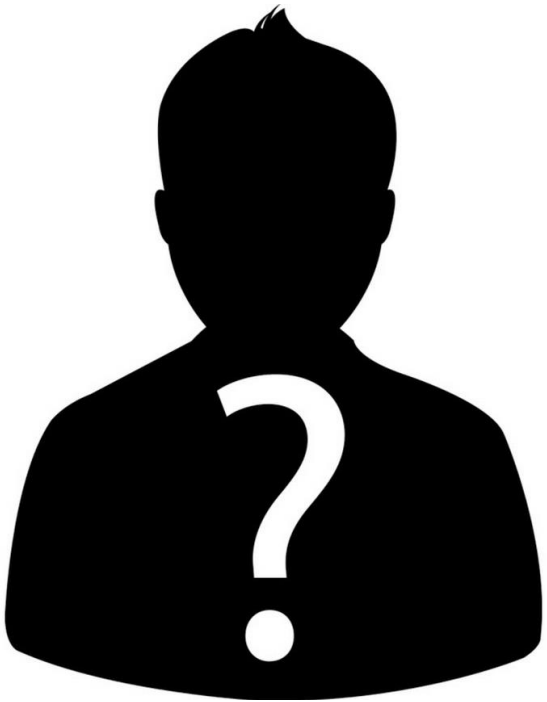
СЗИ от НСД
ViPNet SafePoint

ViPNet SafePoint

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

ViPNet SafePoint устанавливается на рабочие станции и серверы 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

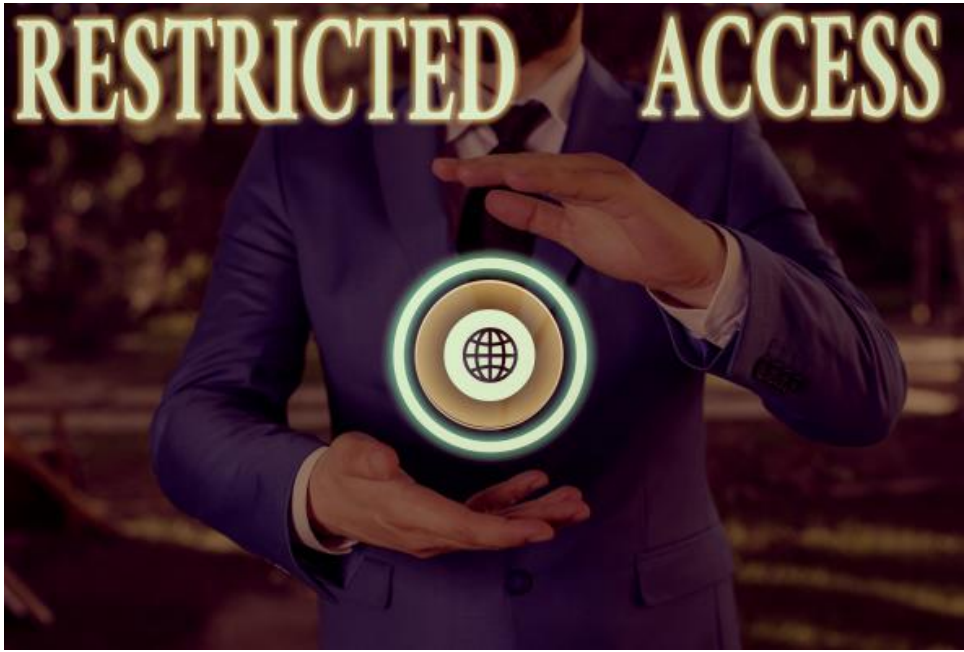
Используем комбинации:

- Логин и пароль
- Логин и идентификатор

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 разрешенные процессы
- Не модифицировал(-ись) важные модули

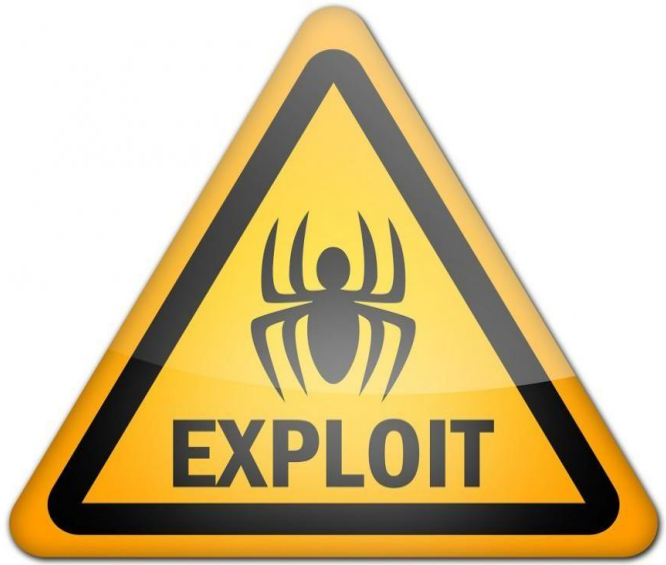


Разграничительные политики для ПО

- 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

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 из 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).

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

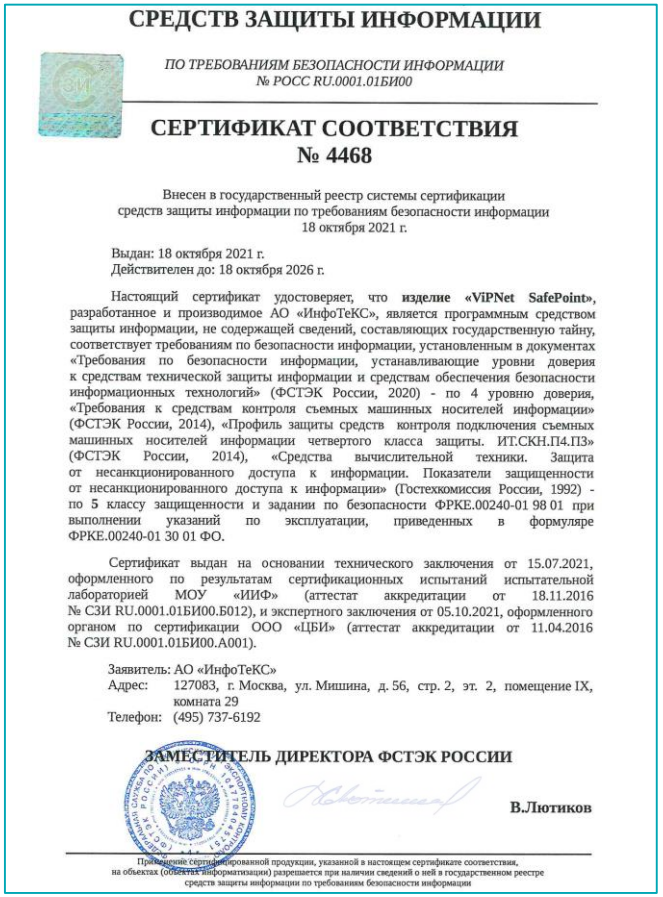
СЗИ от НСД может заменить

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

Доверяй, но проверяй

В последние годы ФСТЭК России проделал огромную работу в направлении «Доверия».

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий от 2020г.



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

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news