Импортозамещение. Комплексные решения вопросов ИБ на рабочих местах

Кадыков Иван
Руководитель продуктового направления

Законодательство

- Единый реестр отечественного ПО
- Ужесточение требований по применению иностранного ПО и оборудования в КИИ
- Постановление правительства №878 от 10.07.2019 «О мерах стимулирования производства радиоэлектронной продукции на территории РФ»
- Единый реестр отечественной радиоэлектронной продукции

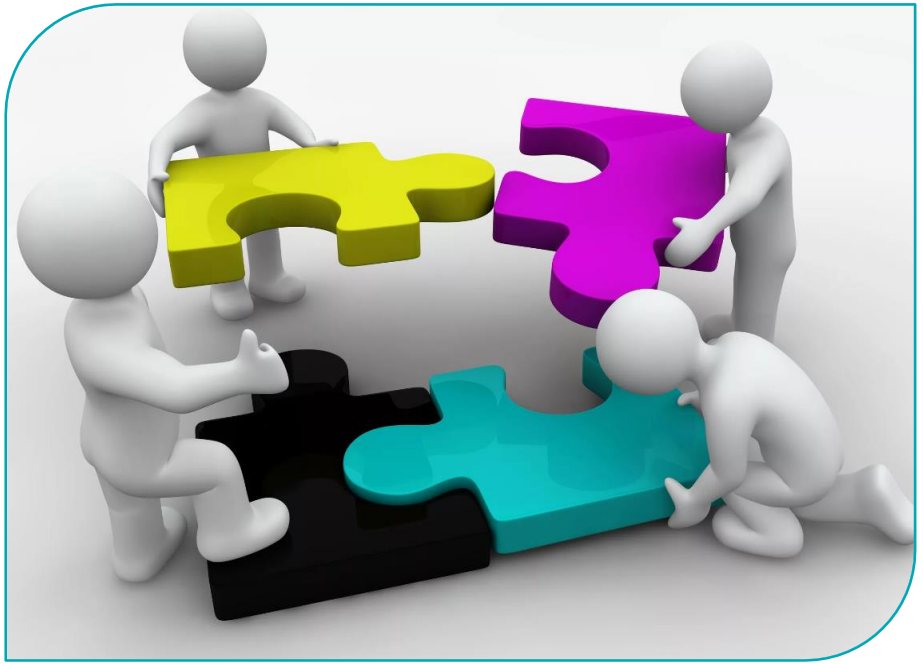
Построение корпоративной системы информационной безопасности чаще всего начинается с обеспечения защиты рабочих станций

Рабочие станции – первичные цели атак

Защита рабочих станций это комплекс мер и задач

При построении автоматизированных систем и подхода к защите рабочих станций всегда решается несколько задач

- Построение автоматизированных систем по требованиям к ИСПДн, ГИС, АСУ ТП и КИИ
- Построение систем по требованиям ФСБ России (СКЗИ, АК, подключение и отправка событий в ГосСОПКА)
- Построение систем с нулевым доверием (ZTNA)
- Защита от продвинутых, бесфайловых и сложных атак
- Построение защищенного канала между пользователями



Комплексное решение для обеспечения соответствия требованиям к СКЗИ класса КС3

ViPNet Client 4U for Linux

- Версия ПО: 4.8 и старше
- Используется виртуальный TUN\TAP интерфейс
- Поддержка широкого списка современных ОС Linux
- Не зависит от версии ядра ОС
- Поддерживает двухфакторную авторизацию
- Поддержка архитектур x86, ARM, Байкал (MIPSel), Эльбрус (e2k)

Имеет сертификаты на соответствие требованиям ФСБ России к СКЗИ классов КС1, КС2 и КС3.

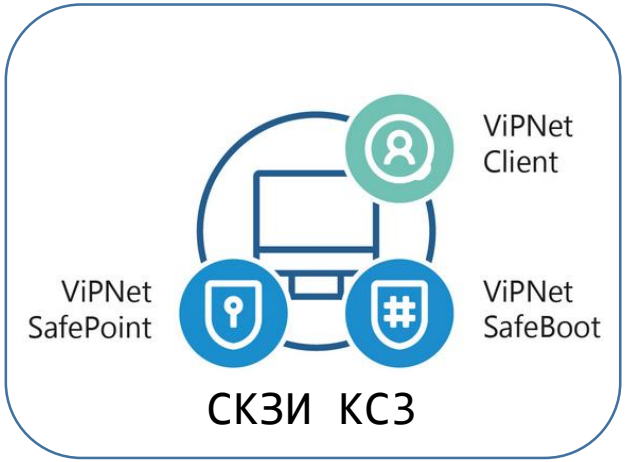
Поддержка ОС Linux в сертифицированной версии

Архитектура	Дистрибутив Linux
x86-64	Astra Linux Special Edition 1.6, 1.7 (РУСБ.10015-01), Common Edition 2.12 «Орел» ГосЛинукс ІС5, РЕД ОС 7.2, 7.3 Альт Рабочая станция 8 СП, 9, 10, К 10 AlterOS 7.5, СинтезМ 7.5, Основа 2.5.2, ЛОТОС, РОСА «КОБАЛЬТ», EMIAS OS 1.0 Ubuntu 18.04.2 LTS, 22.04 LTS, Debian 9.9 CentOS 7.1, 7.5, 8
«Байкал-Т1» (mipsel)	Astra Linux Special Edition 6.1 «Севастополь»
«Эльбрус» (e2k)	Astra Linux Special Edition «Ленинград»
ARMv5	OpenWrt Chaos Calmer
ARMv7	Astra Linux Special Edition «Новороссийск» Сборки для микроконтроллеров на Debian и OpenEmbedded

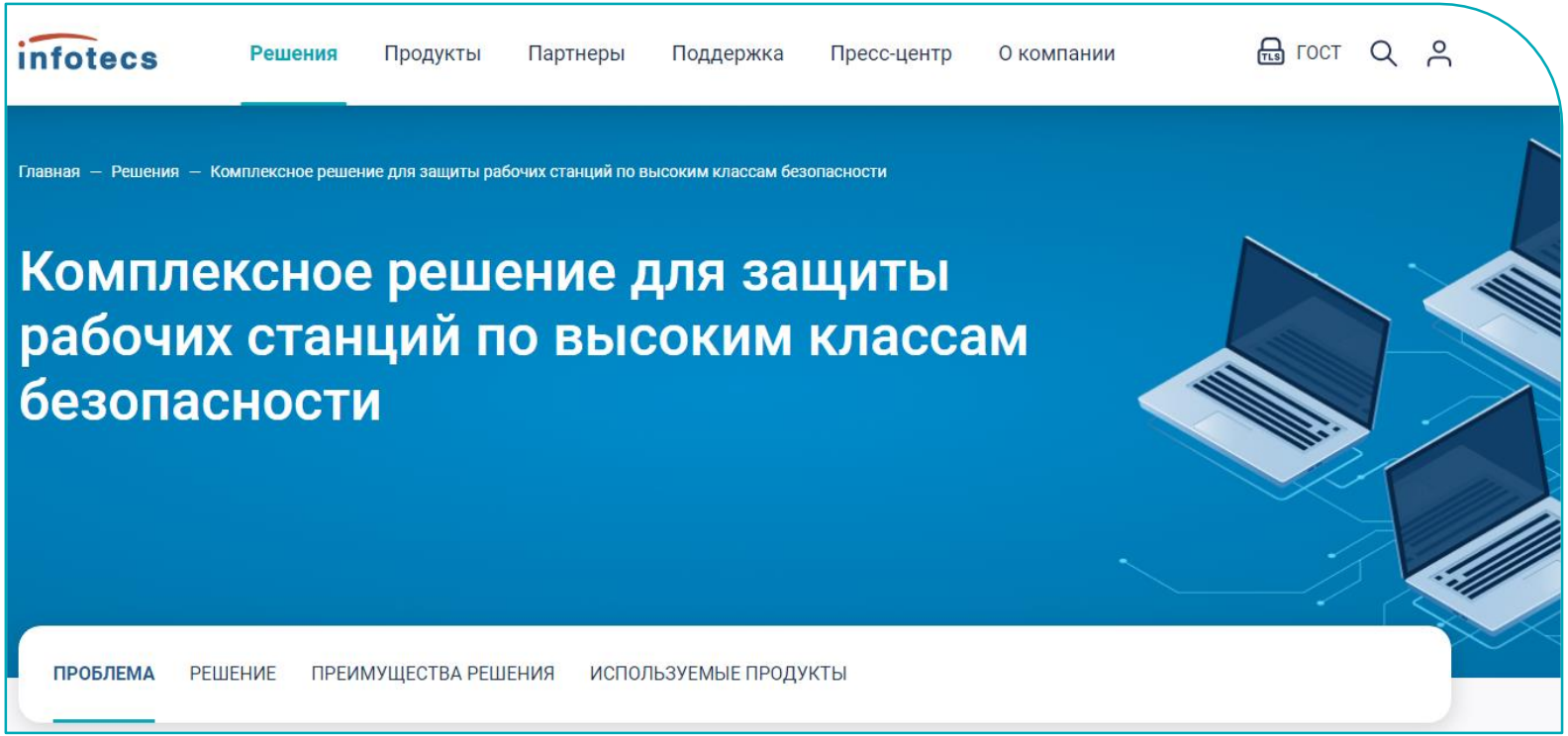
В рамках ИИ обновлён формуляр:

– аппаратно-программный модуль доверенной загрузки либо средство защиты информации, реализующее механизмы доверенной загрузки, имеющие действующие сертификаты ФСБ России, для соответствия требованиям, установленным для классов защиты КС2 и КС3 (исполнения 2 и 3 соответственно);

Схема комплексного решения



Опубликовано описание решения



ViPNet Client 4U for Linux

ТЕХНО 2024 infotecs ФЕСТ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3864 от "23" июля 2020 г.

Действителен до "23" июля 2023 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что программный комплекс **ViPNet Client 4U for Linux** (исполнения 1, 2) в комплектации согласно формуляру ФРКЕ.00239-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2) и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление имитовставки для файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика) информации, не содержащей сведений, составляю[illegible] государственную тайну.

Сертификат выдан на основании результатов проведенных [illegible] ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции [illegible]

Безопасность информации обе[illegible] в соответствии с требованиями эксплуатационно[illegible] E.00239-01 30 01 ФО.

За[illegible] научно-те[illegible]ческой [illegible] защиты информации [illegible] России — О.В. Скрябин

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 23 июля 2020 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России — В.Н. Мартынов

Единый реестр нотификаций о характеристиках шифровальных (криптографических) средств и товаров, их содержащих

Номер нотификации	RU0000049797
Дата публикации нотификации	22.10.20[illegible]
Идентификатор	000000[illegible]
Но[illegible]	RU0000[illegible]9797
[illegible]аименование товара	Программный комплекс ViPNet Client 4U for Linux
[illegible]аименование товара полное	Программный комплекс ViPNet Client 4U for Linux
Изготовитель товара	ОАО "ИнфоТеКС", 127287, Москва, Старый Петровско-Разумовский проезд, д.1/23, стр. 1, тел.8 (495) 737-61-92, факс 8 (495) 793-72-78, e-mail: soft@infotecs.ru, http//infotecs.ru/
Срок действия	30.07.2030
Статус	Действует
Дата аннулирования	
Дата регистрации нотификации	14.10.2020

Сертификаты до 31.05.2025

ViPNet Client 5

Важно!!!

ViPNet Client 4U + iplir 6 = ViPNet Client 5

А это значит, что совместимость с **ViPNet Administrator** и работа на протоколе **iplir 4.1** обеспечена

ViPNet Client 5 for Linux передан на сертификацию в **СФБ Лаб** для подтверждения соответствия требованиям ФСБ России к СКЗИ классов **КС1**, **КС2** и **КС3**

Построение автоматизированных систем по требованиям к ИСПДн, ГИС, АСУ ТП и КИИ

Что главное при построении АС по требованиям ФСТЭК России?

1. Определить под какие требования попадает АС
    1. ИСПДн
    2. ГИС
    3. АСУ ТП
    4. КИИ

2. Посмотреть на огромное количество мер приказов необходимых для закрытия
3. ~~Ужаснуться~~ ☺

Не всё так страшно

- Мер в приказах много, но не все они должны закрываться техническими средствами (есть организационно штатные меры)
- Не все меры могут относиться к целевой АС (всё зависит от класса/уровня защищённости и модели нарушителя)

ГИС, ИСПДн, АСУ ТП, КИИ

Чтобы полностью защитить компьютер, недостаточно иметь одно СЗИ

Количество СЗИ определяется

Моделью нарушителя

Доступной функциональностью (классом продукта)

МДЗ УБ или БСВВ
СЗИ от НСД
СОВ/СПВ
МЭ
АВЗ
АНЗ
Защита канала связи

Какие ключевые меры закрывает каждый продукт

МДЗ

Блок мер ИАФ, УПД

Важное – УПД.3/17

СЗИ от НСД

Блок мер ИАФ, УПД, ОЦЛ

Очень много важного

СОВ/СПВ

Блок мер СОВ и РСБ

Важное – СОВ.1 и СОВ.2

МЭ

Блок мер ЗИС

Важно ЗИС.7/23 и ЗИС.22/34

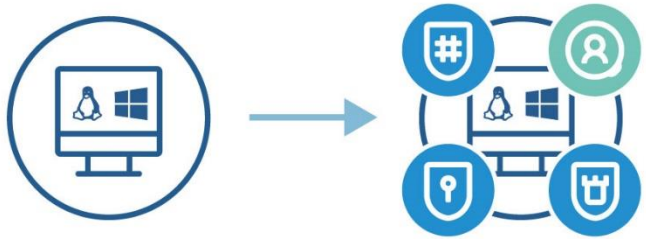
САВЗ/АНЗ

Блок мер АВЗ и АНЗ

Защита канала связи (VPN)

Важно ЗИС.4/20

Комплексное решение для защиты ИСПДн, ГИС, АСУ ТП и КИИ



МДЗ УБ или БСВВ	ViPNet SafeBoot
СЗИ от НСД	ViPNet SafePoint
СОВ/СПВ	ViPNet EndPoint Protection
МЭ	ViPNet EndPoint Protection
АВЗ	ViPNet EndPoint Protection+АВЗ
АНЗ	АНЗ
Защита канала связи	ViPNet Client 4U/5

Таблица 1 – Реализация ViPNet EPP мер по защите информации

№ п/п	Содержание меры по обеспечению безопасности в [1], [2] и ее условное обозначение	Содержание меры по обеспечению безопасности в [3], [7] и ее условное обозначение
1.	ИАФ.1* Идентификация и аутентификация пользователей, являющихся работниками оператора	ИАФ.1* Идентификация и аутентификация пользователей и инициируемых ими процессов
2.	ИАФ.3* Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	ИАФ.3* Управление идентификаторами
3.	ИАФ.4* Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	ИАФ.4* Управление средствами аутентификации
4.	ИАФ.5* Защита обратной связи при вводе аутентификационной информации	В [3], [7] отсутствует соответствующая мера
5.	УПД.1* Управление (заведение, активац блокирование и уничтожение) учетных записями пользователей, в том числе внеш пользователей	
6.	УПД.2 Реализация необходимых метод (дискреционный, мандатный, ролевой и иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	
7.	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений однонаправленная передача и иные спос управления) информационными потока между устройствами, сегментами информационной системы, а также меж информационными системами	
8.	УПД.4* Разделение полномочий (роле пользователей, администраторов и ли обеспечивающих функционирование информационной системы	

2.3.2 ViPNet SafeBoot соответствует 2 классу защиты средств доверенной загрузки (далее – СДЗ), 2 уровню доверия и предназначен для использования:

– в государственных информационных системах до класса защищенности[3] К1 включительно, в информационных системах персональных данных для обеспечения уровня защищенности[4] персональных данных до 1 уровня включительно, в ИС общего пользования II класса[5], в том числе для обеспечения базовых и адаптированных мер защиты информации в соответствии с требованиями, утвержденными приказами ФСТЭК России №17 от 11.02.2013, №21 от 18.02.2013 и №489 от 31.08.2010:

- ИАФ.1* – Идентификация и аутентификация пользователей, являющихся работниками оператора;
- ИАФ.3* – Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- ИАФ.4* – Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- ИАФ.5* – Защита обратной связи при вводе аутентификационной информации;
- УПД.1* – Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- УПД.4* – Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- УПД.6 – Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- УПД.17 – Обеспечение доверенной загрузки средств вычислительной техники;

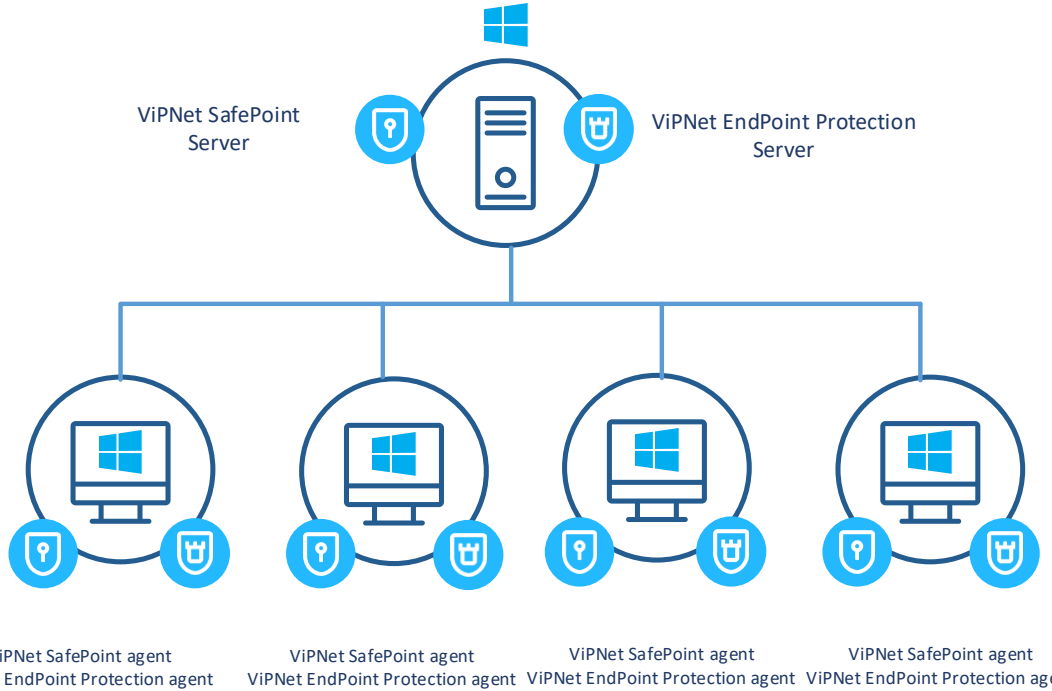
Чтобы вам было проще!

Все меры, которые закрывают продукты, прописаны в Формулярах или Правилах пользования

Импортозамещение

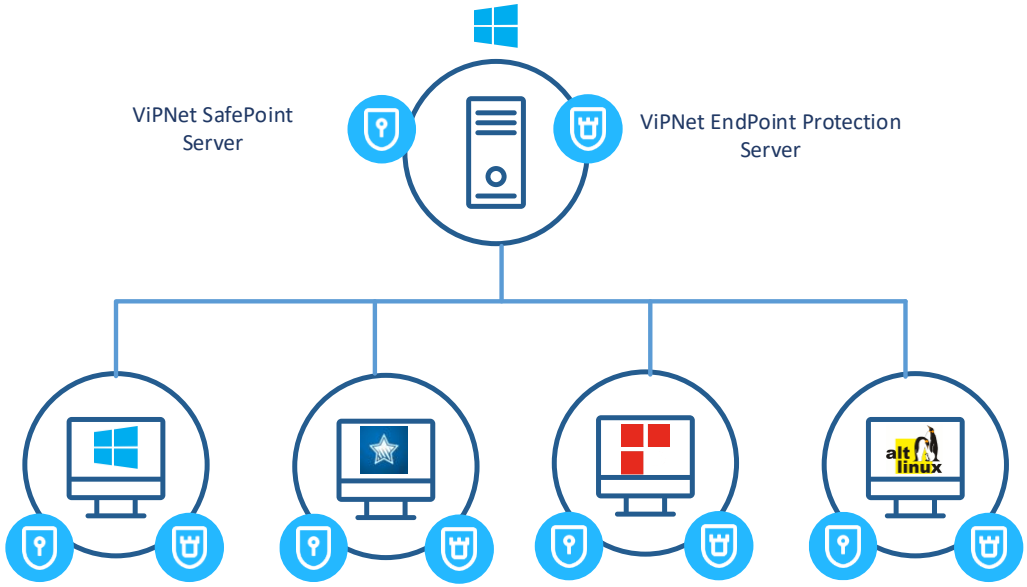
Продукты ViPNet и отечественные ОС

Типичная ситуация до начала импортозамещения



- Клиенты используют Windows
- Все агенты EPP и SP подключены к своим серверам

Переводим часть ПК на отечественные ОС



- Убираем с серверов EPP и SP агентов с Windows-ПК
- Вводим новые компьютеры на отечественной ОС
- Устанавливаем агентов EPP и SP. Подключаем их к серверам.

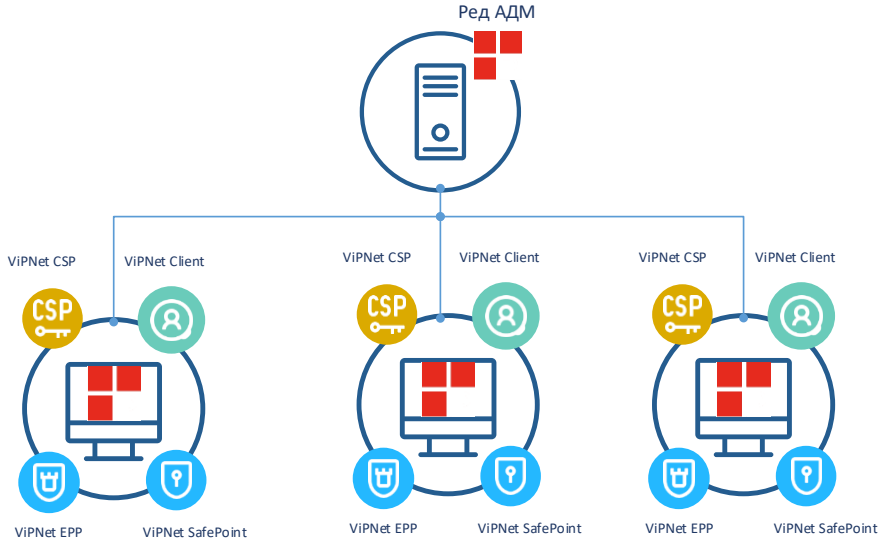
Не нужны новые лицензии!

Варианты развёртывания продуктов с использованием РедАДМ

У нас получилось реализовать установку и обновление тремя вариантами.

Используем стандартную оснастку «Конфигурация → Создать → Редактировать → Параметры →…»:

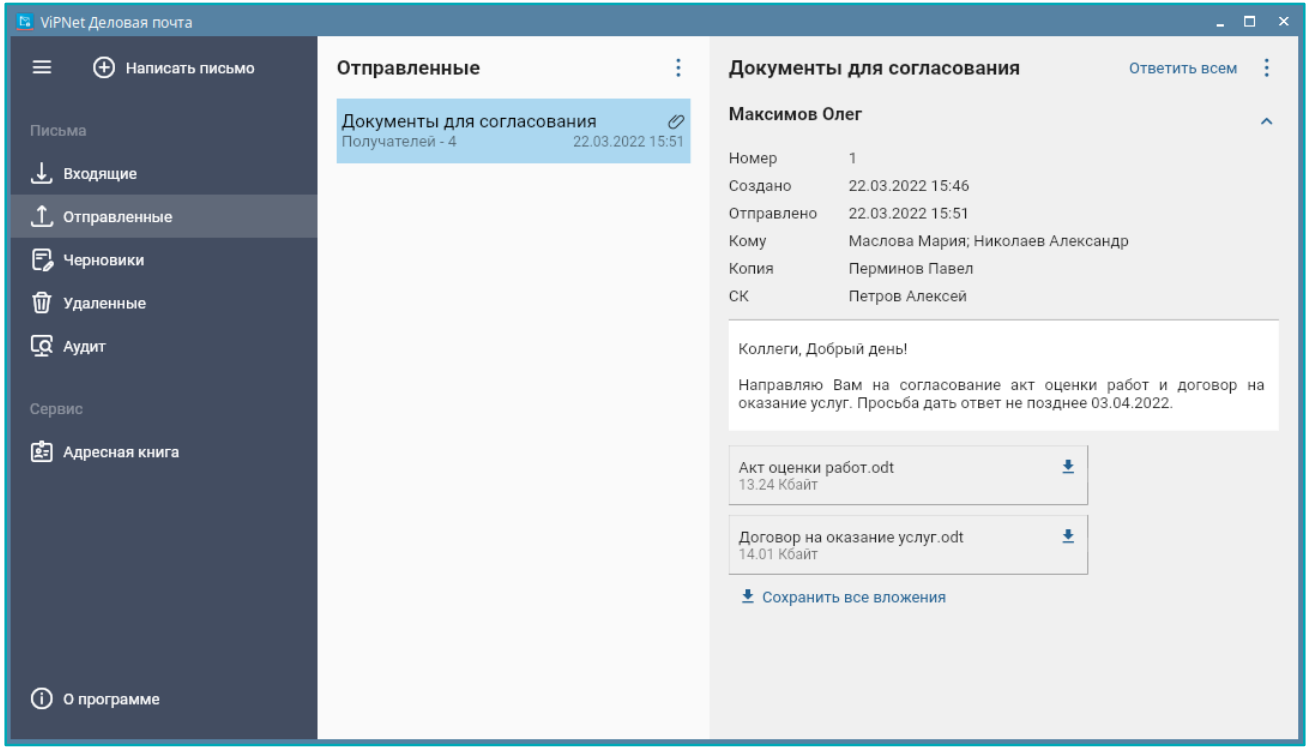
- …Параметры компьютера → Системные настройки → Установка из rpm пакета.
- Параметры компьютера → Системные настройки → Подключение дополнительного репозитория
- Собственные сценарии → Выполнение bash-скрипта



ТЕХНО 2024 infotecs ФЕСТ

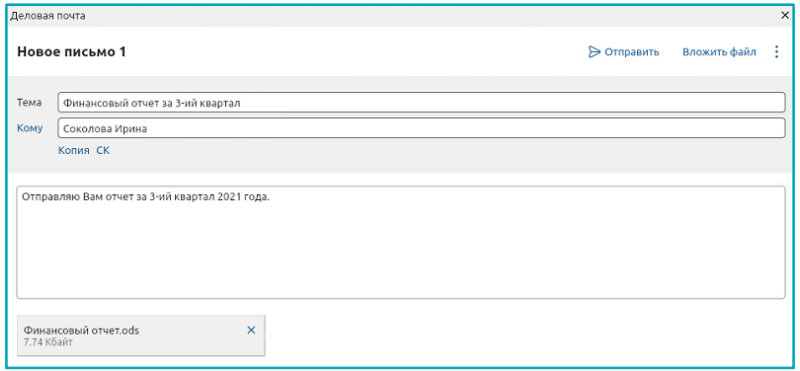
ViPNet Деловая почта

ViPNet Деловая почта для Linux



ViPNet Деловая почта для Linux

- Встречная работа с **ViPNet Деловая почта** для **ОС Windows**
- Поддержка **ОС Linux** из списка поддержки продукта **ViPNet Client 4U for Linux**
- Прикладное шифрование писем и вложений
- Новый UI в современном стиле
- Отдельный модуль автопроцессинга



- Совместимо с **ViPNet Administrator** версии **4.6.10.4916** и старше
- Совместимо с **ViPNet Client 4U for Linux** версии **4.13.1.17762** и старше

ViPNet Деловая почта для Linux

План развития продукта:

- Утилита миграции с ДП Windows на ДП Linux
- Прикладное шифрование писем и вложений при хранении на диске
- Электронная подпись писем и вложений
- Перенос архивов из ДП Windows в ДП Linux
- Поддержка Client 5

ТЕХНО 2024 infotecs ФЕСТ

Кадыков Иван
Руководитель продуктового направления
e-mail: ivan.kadykov@infotecs.ru

Подписывайтесь на наши соцсети