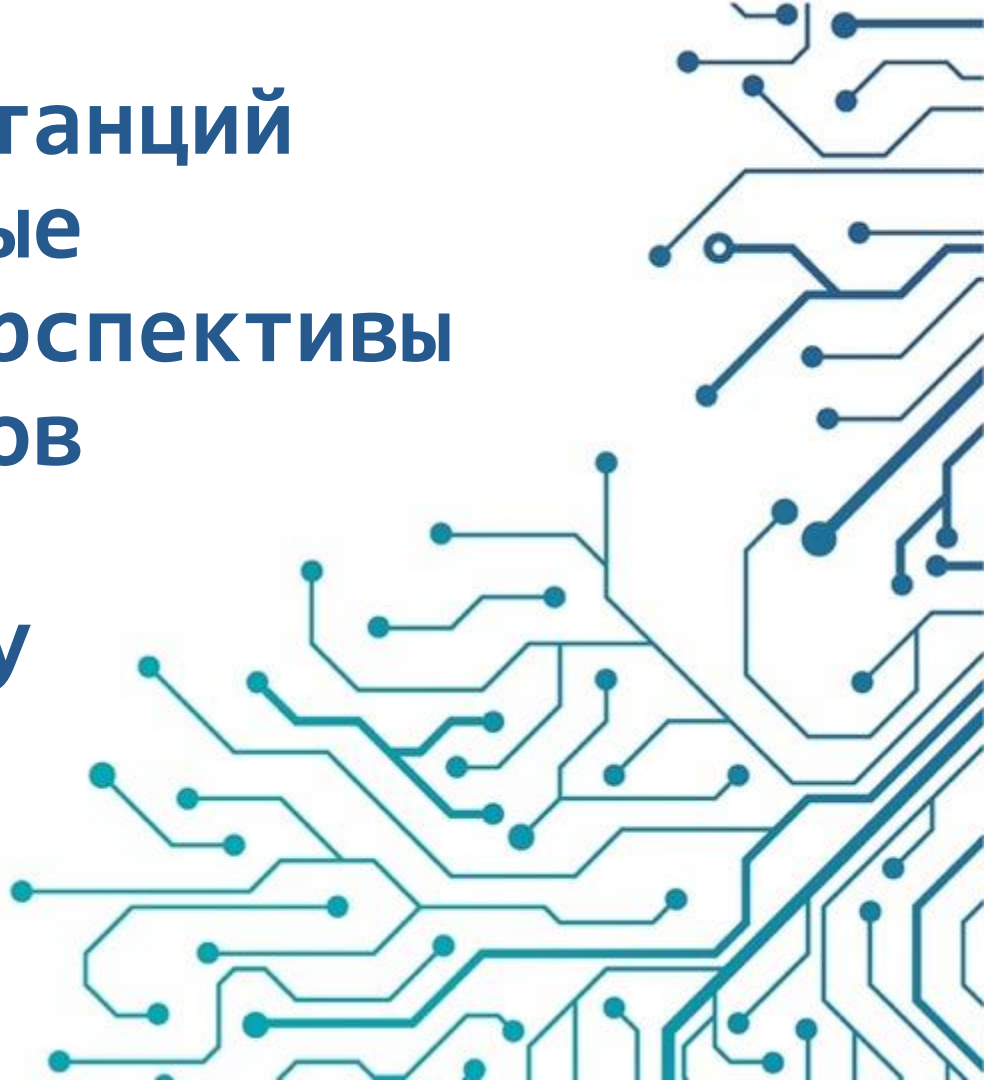


Защита рабочих станций и серверов – новые возможности и перспективы развития продуктов направления Endpoint Security

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.





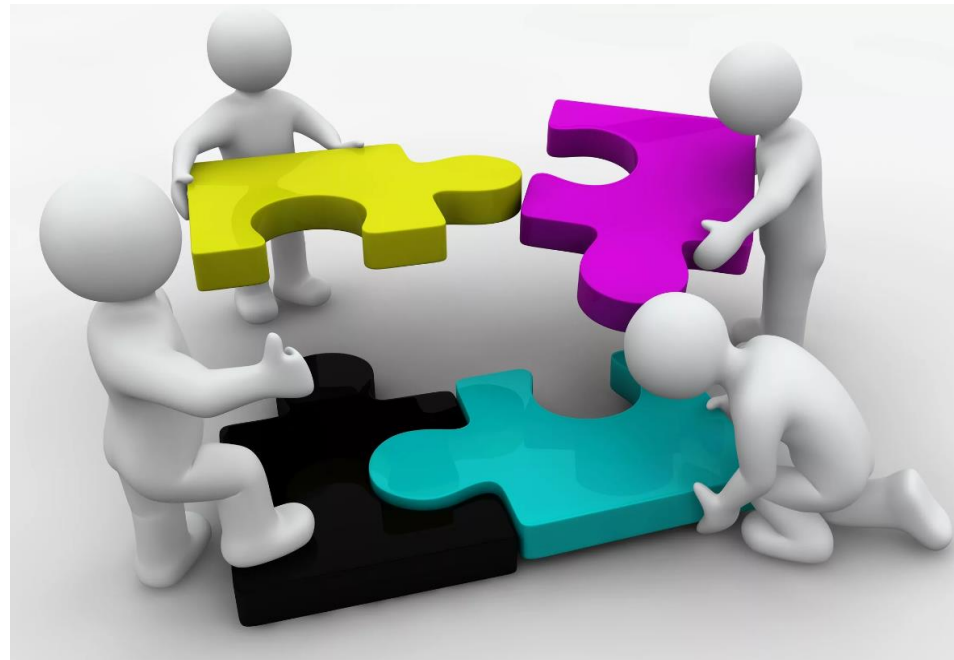
Построение корпоративной системы информационной безопасности чаще всего начинается с обеспечения защиты рабочих станций

Рабочие станции – первичные цели атак

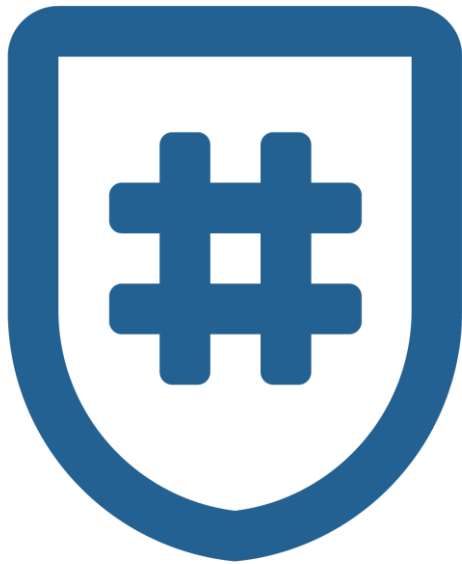
Защита рабочих станций это комплекс мер и задач

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

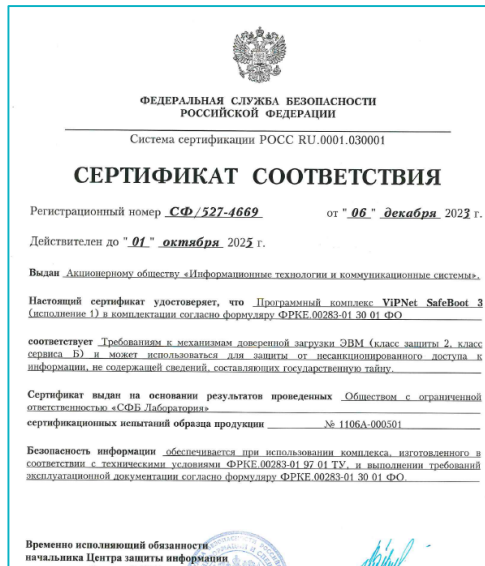
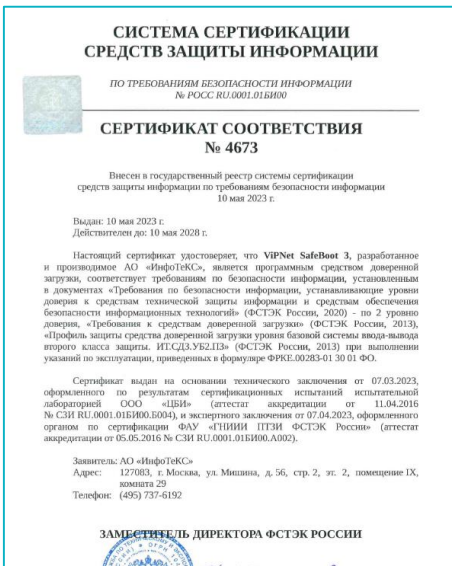


ViPNet SafeBoot 3



Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ). Предназначен для создания точки доверия к платформе и её компонентам, а также к загружаемой операционной системе. Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности и защита компонентов ПК, а также организация доверенной загрузки штатной операционной системы.

VIPNet SafeBoot 3



Сертификаты

- ФСТЭК России № 4673
- ФСБ России № СФ/527-4669

Исполнение 1. VIPNet SafeBoot 3 –
обладает двумя сертификатами
ФСБ России и ФСТЭК России

Исполнение 2. VIPNet SafeBoot 3 –
обладает – только сертификатом
ФСТЭК России

Что даёт сертификат ФСБ России

Возможность использования программного замка ViPNet SafeBoot, вместо аппаратного.

В Формулярах на ViPNet CSP и ViPNet Client уже прописана возможность использования СЗИ МДЗ (Средства защиты информации реализующие механизмы доверенной загрузки II класса, тип сервиса Б.)

Если используете несертифицированную ОС и требуется замкнутая программная среда – ViPNet SafePoint



Общая схема работы

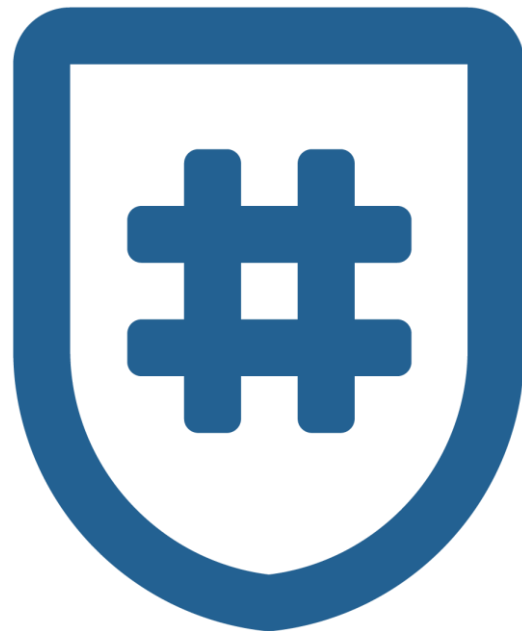


2024 год

- Сертификация версии 3.2 по линии ФСБ, с целью увеличения срока действия сертификата
- Старт работ над релизом 4.0 (что же там будет?)

VIPNet SafeBoot релиз 3.2

- Поддержка syslog – отправка CEF сообщений
- Поддержка ALD PRO (Astra Linux)
- Поддержка работы на бездисковых станциях
- Профили загрузки ОС
- Формирование отчёта о настройках продукта
- Поддержка токена Guardant ID версии 2
- Поддержка JaCarta-2 SE и JaCarta PRO
- Расписание доступа пользователей
- Регистрация всех подключенных устройств аутентификации



Поддержка syslog – отправка CEF сообщений

ViPNet SafeBoot

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация
- Журнал событий**
- БД конфигурации
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Блокировка устройств
- Ключи
- Удаленное управление
- Обновления
- Дополнительно

Перезагрузить систему

Выключить систему

0 продукте

Журнал событий

Режим просмотра и экспорта журнала:

[Просмотреть журнал](#)

[Экспортировать журнал](#)

Режим ведения журнала:

- Подробная регистрация событий
- Журналирование по syslog

IP сервера syslog:

[Настройки фильтра](#)

Заполнение журнала: 3696 из 16426 байт (22%)

Расписание доступа пользователей

ViPNet SafeBoot

- Параметры загрузки ОС
- Контроль целостности
- Аутентификация**
- Журнал событий
- БД конфигурации
- Корневые сертификаты
- Сеть и LDAP
- Регистрация
- Защита
- Блокировка устройств
- Ключи
- Удаленное управление
- Обновления
- Дополнительно

Перезагрузить систему

Выключить систему

О продукте

Аутентификация/Настройки пользователя/Настройки доступа

График работы

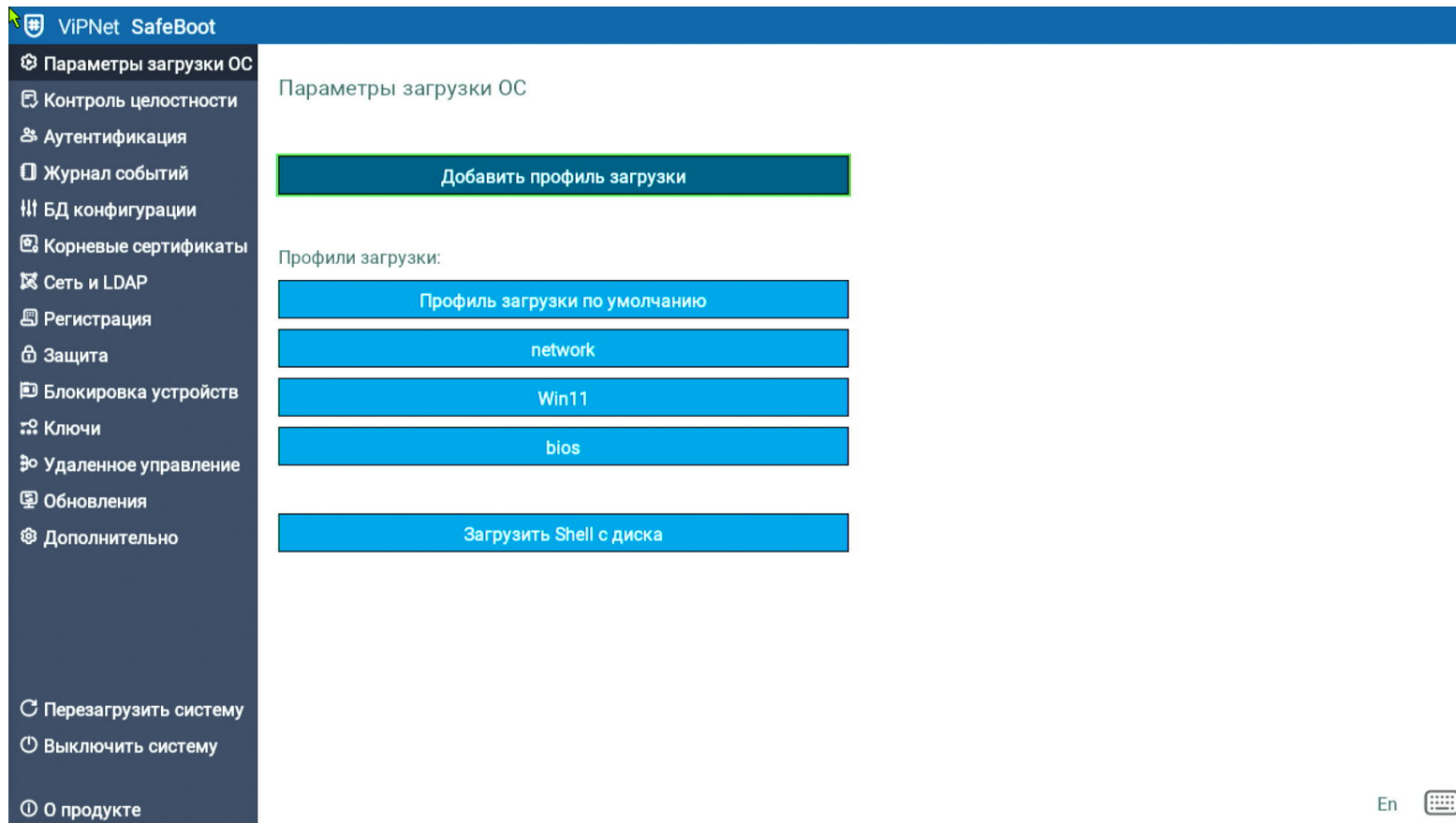
плавающий (2 через 2)

Начало работы (гггг-мм-дд)	2024-11-12
Начало рабочего дня (чч:мм)	09:00
Конец рабочего дня (чч:мм)	18:00
Начало перерыва на обед (чч:мм)	14:00
Конец перерыва на обед (чч:мм)	15:00
Начало ближайшего отсутствия (гггг-мм-дд)	2025-06-01
Конец ближайшего отсутствия (гггг-мм-дд)	2025-06-20

Сбросить настройки доступа



Профили загрузки



The screenshot shows the 'VIPNet SafeBoot' BIOS configuration utility. The left sidebar contains a menu with the following items: 'Параметры загрузки ОС' (highlighted), 'Контроль целостности', 'Аутентификация', 'Журнал событий', 'БД конфигурации', 'Корневые сертификаты', 'Сеть и LDAP', 'Регистрация', 'Защита', 'Блокировка устройств', 'Ключи', 'Удаленное управление', 'Обновления', 'Дополнительно', 'Перезагрузить систему', 'Выключить систему', and 'О продукте'. The main area is titled 'Параметры загрузки ОС' and features a 'Добавить профиль загрузки' button at the top. Below this, under the heading 'Профили загрузки:', there are four buttons: 'Профиль загрузки по умолчанию', 'network', 'Win11', and 'bios'. At the bottom of the main area is a 'Загрузить Shell с диска' button. The bottom right corner of the interface shows 'En' and a keyboard icon.

Получено положительное заключение!

ViPNet SafeBoot 3 (исполнении 1)
соответствует «Требованиям к механизмам
доверенной загрузки ЭВМ» по классу 2Б.

Заключение № 149/3/4/3/1800 от
04.10.2024 действует **до 01.10.2034**



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.



Идентификация и аутентификация

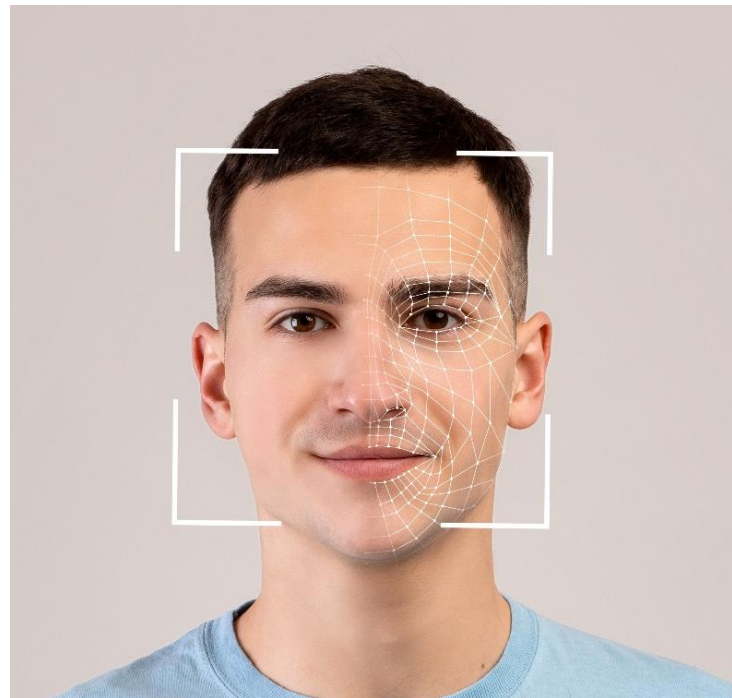
Своих пользователей надо знать
«в лицо», поэтому:

**Идентификация и аутентификация
пользователей** выполняется собственными
механизмами

SSO с ViPNet SafeBoot

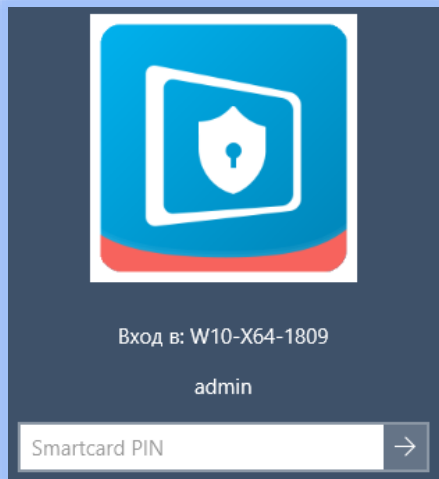
Используем комбинации:

- 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
- Rutoken ЭЦП 3.0
- Rutoken ЭЦП PKI



Создание разграничительных политик для пользователя ЗПС

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



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

Поддерживаемые ОС

Сервер:

- Microsoft Windows 10 (21H2) / 11 (21H2)
- Microsoft Windows Server 2016 (1607) / 2019 (1809)

Агент

- Microsoft Windows 10 (21H2) / 11 (21H2)
- Microsoft Windows Server 2016 (1607) / 2019 (1809)
- Альт Рабочая станция 10.1*
- РЕД ОС 7.3.2(3,4) «Муром»*
- Astra Linux Special Edition 1.7.4*
- Debian 11 (bullseye)*

*т.к. продукт ядрозависимый – ВАЖНО для ОС линукс смотреть на поддержку ядра, она приведена в РА



Что нового в 2024 год

- Выпуск продукта с поддержкой новых ядер отечественных ОС
- Реализован динамический контроль целостности
- Тиражирование настроек для клиентов `linux`



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 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 «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 соответствует,
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



VIPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Защитные механизмы



Система обнаружения и предотвращения вторжений

Обнаруживаем и предотвращаем атаки:

- На уровне ОС
- На уровне сети



Дополнительное в модуле системы обнаружения и предотвращения вторжений

- TLS – инспекция – возможность расшифровывания трафика проходящего через модули ViPNet EndPoint Protection. База «bad URL» поставляется в рамках БП, обновляется регулярно
- SafeBrowsing – безопасный сёрфинг в интернете (веб-фильтрация)



Adminистратор

Редактор правил - Обнаружение и предотвращение вторжений - malware

Поиск по названию фильтра... + Добавить ↑

Название фильтра	Статус	Действие	Журнал
Фильтры политик безопасности			
<input type="checkbox"/> malware	<input checked="" type="checkbox"/>	! Блокировать	ll
<input type="checkbox"/> phishing	<input checked="" type="checkbox"/>	! Блокировать	ll
<input type="checkbox"/> spam	<input checked="" type="checkbox"/>	! Блокировать	ll
Фильтры по умолчанию			
<input checked="" type="checkbox"/> Прочие сайты	<input checked="" type="checkbox"/>	✓ Разрешить	

malware

Фильтрация активна

Наименование фильтра

Действие ! Блокировать

Записывать обращение к URL-адресу в журнал

URL-адреса

ips.csv

domains.csv

urls.csv

domains.csv

Domains

varejaocajuru.com.br

xn--mgb2dlba59cthb.ga

oeuskemv.cn

gsdbdfgwen.top

mizuhobqnk-jp.com

updatewindow.com.

cdncloud.digital.

cloud.cdncach.com.

windows.microsoft-cloud.ml.

service-1kgeq4ma-1253493857.gz.apigw.tencentcs.com.

podcli-jp.life

sezezapa.com.

activeservers.net.

changjiang.online.

hotbox.com

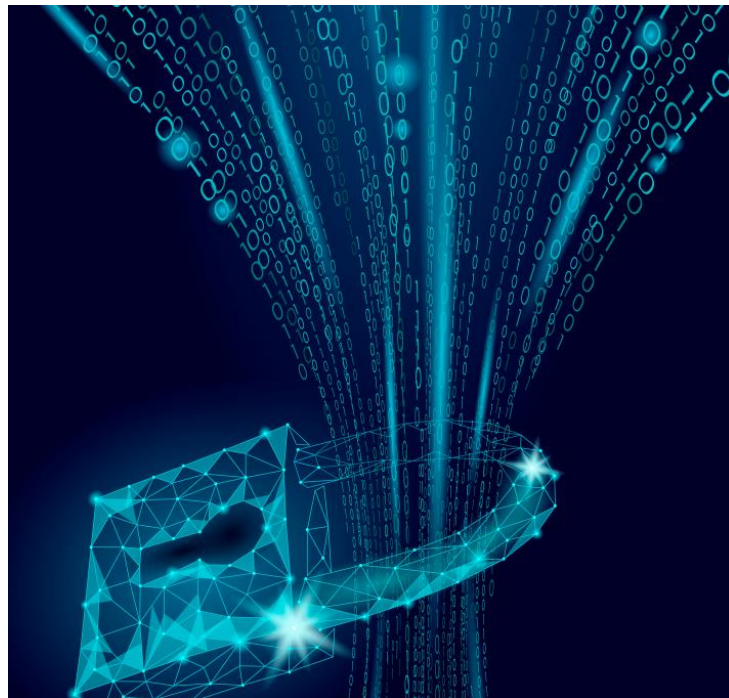
Сохранить Отмена

Как это выглядит

Межсетевой экран

- Фильтрация трафика Ipv4 и Ipv6
- Интеграция с ViPNet Client 4U/5

Добавление\Редактирование\Удаление фильтров защищённой сети из локальной консоли ViPNet EndPoint Protection (агент)



Создание фильтров защищённой сети

ViPNet EPP Администратор

Назад к EndPoint Protection

Персональный межсетевой экран - Фильтры режима работы 'Корпоративная сеть'

Поиск по названию фильтра... Создать фильтр

Название фильтра	Статус	Действие	Версия IP	Протокол	Источник	Назначение	Расписание
Пользовательские фильтры							
<input type="checkbox"/> VPN_filter	<input checked="" type="checkbox"/>	Разрешить	IP v4,v6	Все	Мой компьютер	координаторы	Всегда

Фильтры по умолчанию							
<input checked="" type="checkbox"/> Действие по умолчанию	<input type="checkbox"/>	Разрешить	IP v4,v6	Все	Все	Все	Всегда

Copyright © 2023 Infotecs | Версия ПО: 1.6.0.13122 | База правил: 2.0.2. Обновлено: 02.10.2023 13:32:09

Назад к EndPoint Protection

Основное

- Сведения
- Режимы работы

Средства

- Персональный межсетевой экран
- Контроль приложений
- Обнаружение и предотвращение вторжений
- ZTNA

Редактор правил - ZTNA

Сохранить Отмена

Включить политики ZTNA

Правила

Windows Linux

Название правила	Статус
Наличие работающего антивируса Kaspersky Antivirus	<input checked="" type="checkbox"/> Включено
Наличие работающего антивируса Dr.Web Antivirus	<input type="checkbox"/> Выключено
<input type="text" value="Название правила"/>	
<input type="checkbox"/> Название правила	Статус

Название правила |

Назад к EndPoint Protection

Основное

- Свойства

Параметры агента

- Актуальность базы антивируса
- Службы systemd
- Файлы
- Модули ядра
- Версия ядра

Редактор правил - Наличие работающего антивируса Kaspersky Antivirus

Сохранить Отмена

Правило для агентов Linux

Службы systemd

|

Название	Требуемое состояние	Статус
<input type="checkbox"/> Название		
<input type="checkbox"/> kesl.service	Выполняется	<input checked="" type="checkbox"/> Включено

Службы systemd

Включено

Название

* Имя службы systemd.

Требуемое состояние

Выполняется

Не выполняется

Сохранить Отмена

Настройки для ZTNA

Контроль приложений

- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



Эвристический Antimalware движок

- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП



Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномалия в создании задачи планировщику
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.



Обнаруживаем бесфайловые атаки

В соответствии с классификацией MITRE ATT&CK

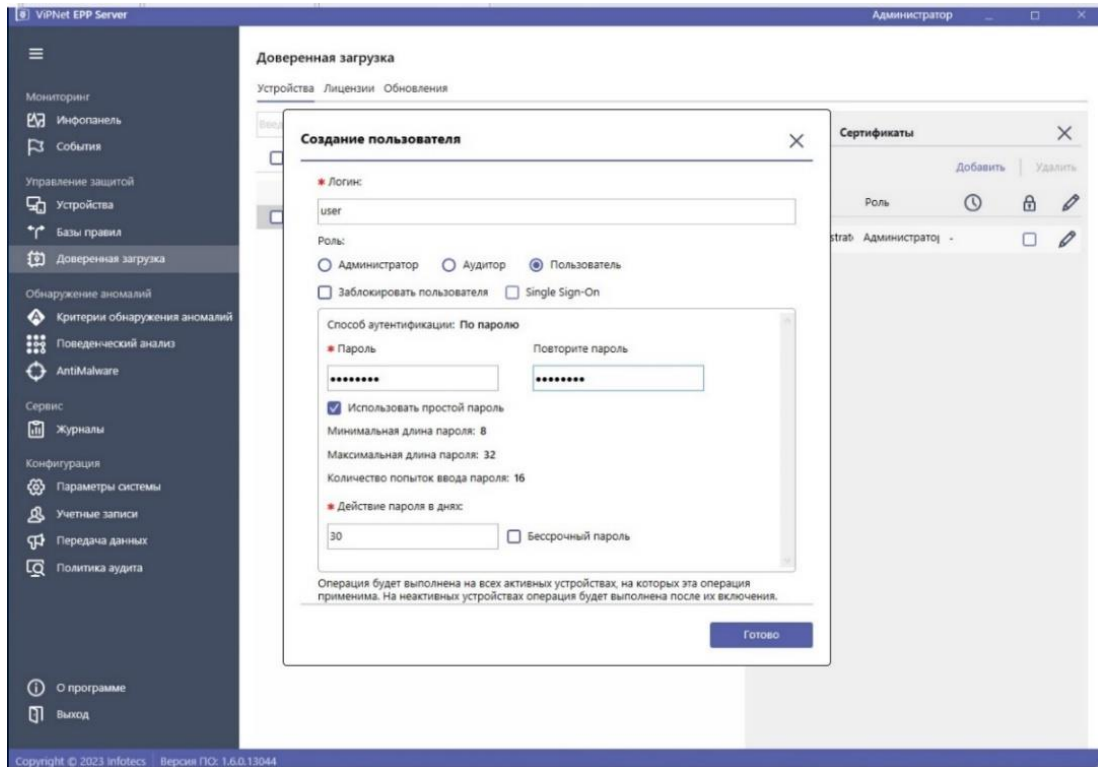
- Credential API Hoocking
- Process Hollowing
- Process Doppelganging
- Dynamic-link library injection
- Portable Executable injection
- Keylogging



Управление ViPNet SafeBoot

Механизмы удалённого управления ViPNet SafeBoot:

- Лицензирование
- Получение журналов
- Обновление МДЗ
- Управление пользователями
- Установка корневых сертификатов



Поддерживаемые ОС

Сервер:

- Microsoft Windows 10 / 11
- Microsoft Windows Server 2016 / 2019 / 2022
- Astra Linux Special Edition 1.7.4

Агент

- Windows Microsoft Windows 8.1 / 10 / (23H2)
- Microsoft Windows Server 2016 / 2019 / 2022
- Альт Рабочая станция 8 / 10 / 10.1*
- РЕД ОС 7.3 / 7.3.2 / 7.3.3 / 7.3.4 «Муром»*
- Astra Linux Special Edition 1.7.4 / 1.7.5*
- Debian 11 (bullseye) / 12 (bookworm)*

*т.к. продукт ядрозависимый – ВАЖНО для ОС линукс смотреть на поддержку ядра, она приведена в РА



Что нового в 2024 году?

Выпуск версии 1.7:

- Standalone-агенты – возможность работы агентов без сервера и поддержка новой модели лицензирования
- UI для Linux агента – ранее у агента был только CLI
- Дополнение функций ZTNA для работы с Client
- Устранение уязвимости в suicata

До конца года выпустим 1.7.1

- Получение фильтров от PMM через 4U/5
- Множественное добавление веб-фильтров
- Дополнительные опции для ZTNA
- Отправка информации о состоянии EPP в ViPNet Client



Агент EPP под Linux – Режимы работы

VIPNet EPP

Режимы работы

- Межсетевой экран** (Firewall)
 - Включено

Корпоративная сеть
Пользователь самостоятельно определяет правила фильтрации трафика. Если правила блокировки не заданы, разрешен любой трафик.

- Обнаружение вторжений** (Intrusion Detection)
- Включено

Правила обнаружения вторжений определяются политикой безопасности EPP. Отключить обнаружение вторжений нельзя.
- Предотвращение вторжений** (Intrusion Prevention)
- Включено

Оптимальный режим
Используется оптимальный набор правил предотвращения вторжений, обеспечивающий достаточную защиту в большинстве случаев.

Сайдбар меню:

- Мониторинг
 - Режимы работы
 - События
 - Соединения
 - Трафик
- Политики
 - Межсетевой экран
 - Фильтры политик безопасности
 - Справочники
 - Обнаружение вторжений
 - Предотвращение вторжений
 - Обнаружение аномалий
 - Импорт и экспорт базы правил
- Система
 - Самотестирование
 - Журнал аудита
 - Учётные записи
 - Настройки
 - О программе
 - Выйти

Агент EPP под Linux – HIPS, правила и их редактирование

VIPNet EPP x

- ☰
- Мониторинг
- 📄 Режимы работы
- 📅 События
- 🔗 Соединения
- 📊 Трафик
- Политики
- 🛡️ Межсетевой экран
 - Фильтры политик безопасности
 - Справочники
- 🗨️ Обнаружение вторжений
- 🗨️ Предотвращение вторжений
- 🔍 Обнаружение аномалий
- 📁 Импорт и экспорт базы правил
- Система
- 🔄 Самотестирование
- 📖 Журнал аудита
- 📄 Учётные записи
- ⚙️ Настройки
- 📄 О программе
- 🚪 Выйти

Предотвращение вторжений

Правила анализа сетевых событий

Усиленный режим
Оптимальный режим
Минимальный режим

🔍 Редактировать файл правил

Идентификатор	Правило	Состояние	Адрес источника	Порт источника	Адрес назна
3307536	AM EXPLOIT Possible Apache HTTP Server v2.4.53 DoS (CVE-2022-30522)	● Включено	Любой	Любой	\$HOME_NET
3307493	AM EXPLOIT Joomla v4.0.0-v4.2.7 Information Disclosure (CVE-2023-23752)	● Включено	\$EXTERNAL_NET	Любой	\$HOME_NET
3307492	AM EXPLOIT HyperSQL (hsqldb) < v2.7.1 RCE (CVE-2022-41853)	● Включено	Любой	Любой	\$HOME_NET
3307491	AM EXPLOIT Possible Apache Commons FileUpload < v1.5 DoS (CVE-2023-...	● Включено	Любой	Любой	\$HOME_NET
3307490	AM EXPLOIT Possible Apache Tomcat v8.5.0 - v11.0.0 HTTP Request Smug...	● Включено	Любой	Любой	\$HOME_NET
3307489	AM EXPLOIT Cacti <= v1.2.24 SQLi via 'automation_networks.php' (CVE-202...	● Включено	Любой	Любой	\$HOME_NET
3307488	AM EXPLOIT Cacti <= v1.2.24 SQLi via 'vdef.php' (CVE-2023-39357)	● Включено	Любой	Любой	\$HOME_NET
3307486	AM EXPLOIT Cacti <= v1.2.24 SQLi via 'user_admin.php' (CVE-2023-39357)	● Включено	Любой	Любой	\$HOME_NET
3307485	AM EXPLOIT Cacti <= v1.2.24 SQLi via 'color_templates.php' (CVE-2023-393...	● Включено	Любой	Любой	\$HOME_NET
3307470	AM EXPLOIT Possible ImageMagick v7.1.0-49 Information Disclosure via B...	● Включено	\$EXTERNAL_NET	Любой	\$HOME_NET
3306445	AM EXPLOIT Possible Google Chrome < v100.0.4896.75 V8 Type Confusion...	● Включено	\$EXTERNAL_NET	Любой	\$HOME_NET
3297325	AM EXPLOIT Apache Kylin v2.0.0 - v4.0.1 RCE (CVE-2022-24697)	● Включено	Любой	Любой	\$HOME_NET
3297324	AM EXPLOIT Markdown Preview Enhanced v0.6.5 - v0.19.6 Command Injec...	● Включено	\$EXTERNAL_NET	Любой	\$HOME_NET
3297322	AM EXPLOIT Sandbox Escape in Debian Redis v5.5.0.3-4+deb10u1 - v5.6.0...	● Включено	Любой	Любой	\$HOME_NET
3297203	AM EXPLOIT Possible WordPress Limit Login Attempts Plugin < v1.7.2 Stor...	● Включено	Любой	Любой	\$HOME_NET
3297202	AM EXPLOIT Generic Possible XSS in HTTP 'Cookie' Header: 'onload' in req...	● Включено	Любой	Любой	\$HOME_NET
3297200	AM TROJAN Ransom.Linux/TARGETCOMP Ransomware payload Downloa...	● Включено	\$HOME_NET	Любой	\$EXTERNAL_N
3297199	AM TROJAN Possible Ransom.Linux/TARGETCOMP Data Exfiltration Attem...	● Включено	\$HOME_NET	Любой	\$EXTERNAL_N
3297186	AM EXPLOIT WordPress HTML5 Video Player Plugin <= v2.5.26 SQLi (CVE-...	● Включено	Любой	Любой	\$HOME_NET
3296781	AM EXPLOIT Possible AVideo WWBIndex v12.4-v14.2 RCE (CVE-2024-318...	● Включено	\$EXTERNAL_NET	Любой	\$HOME_NET
3296681	AM EXPLOIT Possible Zoho ManageEngine ADSelfService Plus < v6218 Do...	● Включено	Любой	Любой	\$HOME_NET

Агент EPP под Linux – Межсетевой экран

VIPNet EPP

Меню

- Мониторинг
 - Режимы работы
 - События
 - Соединения
 - Трафик
- Политики
 - Межсетевой экран ^
 - Фильтры политик безопасности**
 - Справочники
 - Обнаружение вторжений
 - Предотвращение вторжений
 - Обнаружение аномалий
 - Импорт и экспорт базы правил
 - Система
 - Самотестирование
 - Журнал аудита
 - Учётные записи
 - Настройки
 - О программе
 - Выйти

Фильтры политик безопасности

Корпоративная сеть | Частная сеть

Поиск Создать фильтр ▾

Фильтр	Состояние	Действие	Тип фильтра	Версия IP	Источники	Назначения	Протокол
▼ 🔒 Фильтры политик безопасности							
▼ <input type="checkbox"/> Пользовательские фильтры							
<input type="checkbox"/> Веб-серфинг	● Включено	⊕ Пропускать	Открытой сети	IPv4	Любые	Любые	DHCP, I
<input type="checkbox"/> Почта	● Включено	⊕ Пропускать	Открытой сети	IPv4	Любые	Любые	IMAP, P
<input type="checkbox"/> Исходящие RDP подключения	● Включено	⊕ Пропускать	Открытой сети	IPv4	Мой компьютер	Любые	RDP
<input type="checkbox"/> Входящие RDP подключения	● Включено	⊕ Пропускать	Открытой сети	IPv4	Другие компьютеры	Мой компьютер	RDP
▼ 🔒 Системный фильтр							
<input checked="" type="checkbox"/> Действие по умолчанию	● Включено	⊖ Блокировать	Открытой сети	IPv4, IPv6	Любые	Любые	Любые

Агент EPP под Linux – Журнал событий

VIPNet EPP

События

Поиск: 11.2024 00:00 – 12.11.2024 23:59

<input type="checkbox"/>	Дата и время	Уровень события	Событие
<input type="checkbox"/>	12.11.2024 16:58:10	Информационное	Обнаружено использование утилиты 'nmap', связанной с сетевым сканированием
<input type="checkbox"/>	12.11.2024 16:57:33	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:33	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:32	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:32	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:32	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:32	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:32	Критическое	Установка deb пакета
<input type="checkbox"/>	12.11.2024 16:57:30	Важное	Обнаружена успешная аутентификация под 'root'
<input type="checkbox"/>	12.11.2024 16:57:30	Важное	Выполнение sudo команды
<input type="checkbox"/>	12.11.2024 16:57:11	Важное	Изменение файла /etc/hosts
<input type="checkbox"/>	12.11.2024 16:57:04	Важное	Обнаружена успешная аутентификация под 'root'
<input type="checkbox"/>	12.11.2024 16:57:04	Важное	Выполнение sudo команды
<input type="checkbox"/>	12.11.2024 16:56:11	Важное	Сервис был запущен
<input type="checkbox"/>	12.11.2024 16:56:06	Критическое	Сервис был остановлен
<input type="checkbox"/>	12.11.2024 16:56:06	Важное	Сервис был запущен
<input type="checkbox"/>	12.11.2024 16:56:06	Критическое	Сервис был остановлен
<input type="checkbox"/>	12.11.2024 16:56:06	Важное	Сервис был запущен
<input type="checkbox"/>	12.11.2024 16:56:06	Критическое	Сервис был остановлен
<input type="checkbox"/>	12.11.2024 16:56:06	Важное	Сервис был запущен
<input type="checkbox"/>	12.11.2024 16:56:05	Критическое	Сервис был остановлен
<input type="checkbox"/>	12.11.2024 16:56:05	Важное	Сервис был запущен
<input type="checkbox"/>	12.11.2024 16:56:05	Критическое	Сервис был остановлен
<input type="checkbox"/>	12.11.2024 16:56:05	Важное	Сервис был запущен

Обнаружено использование утилиты "nmap", связанной с сетевым сканированием

Общие

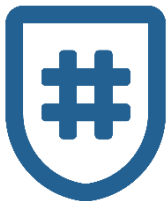
Событие	Обнаружено использование утилиты 'nmap', связанной с сетевым сканированием
Уровень события	Информационное
Дата и время	12.11.2024 16:58:10
Категория угрозы	Подозрительная, потенциально опасная активность
Тип правила	Системная активность
Версия базы правил	1.7.1.13
Модуль	Обнаружение вторжений

Показывать в виде текста события

Событие 1

Обнаружено использование утилиты 'nmap', связанной с сетевым сканированием

Endpoint Security



ViPNet SafeBoot 3



ViPNet Client



ViPNet SafePoint



ViPNet EndPoint Protection



Курс
«Администрирование
средств защиты ViPNet
EndPoint Protection, ViPNet
SafeBoot, ViPNet SafePoint»

-30%

Администрирование системы защиты информации ViPNet EndPoint Protection, ViPNet SafeBoot, ViPNet SafePoint

[Вернуться к списку](#)

Код: ОК038

49 500.00 рублей

ЗАПИСАТЬСЯ НА КУРС

Ближайшие курсы

23.12.2024 - 27.12.2024

03.03.2025 - 07.03.2025

Форма обучения: очная **с отрывом от работы.**

Учебных часов по программе: 40 академических часов.

Режим обучения: 5 рабочих дней по 8 академических часов в день. Обучение проходит с 10.00 ч. до 17.00 ч. по московскому времени.

Подписывайтесь
на наши соцсети,
там много интересного




infotecs

The logo for 'infotecs' features a red curved line above the word 'infotecs' in a bold, dark blue, sans-serif font.

Спасибо за внимание!