ViPNet SafeBoot 3
– доверие, безопасность и технологическое превосходство

БОЛЬШОЙ МОСКОВСКИЙ ТЕХНО infotecs ФЕСТ

Иван Кадыков
руководитель продуктового направления

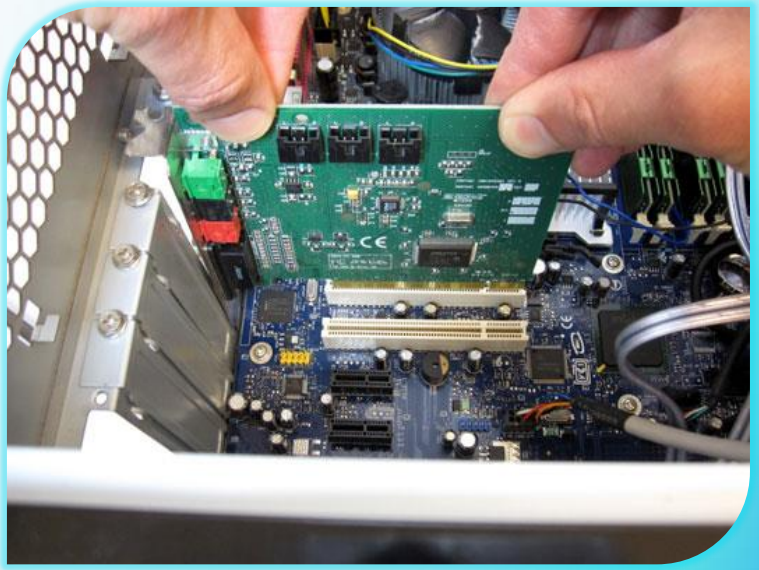
Доверенная загрузка – первый и ключевой шаг к защите рабочих станций и серверов

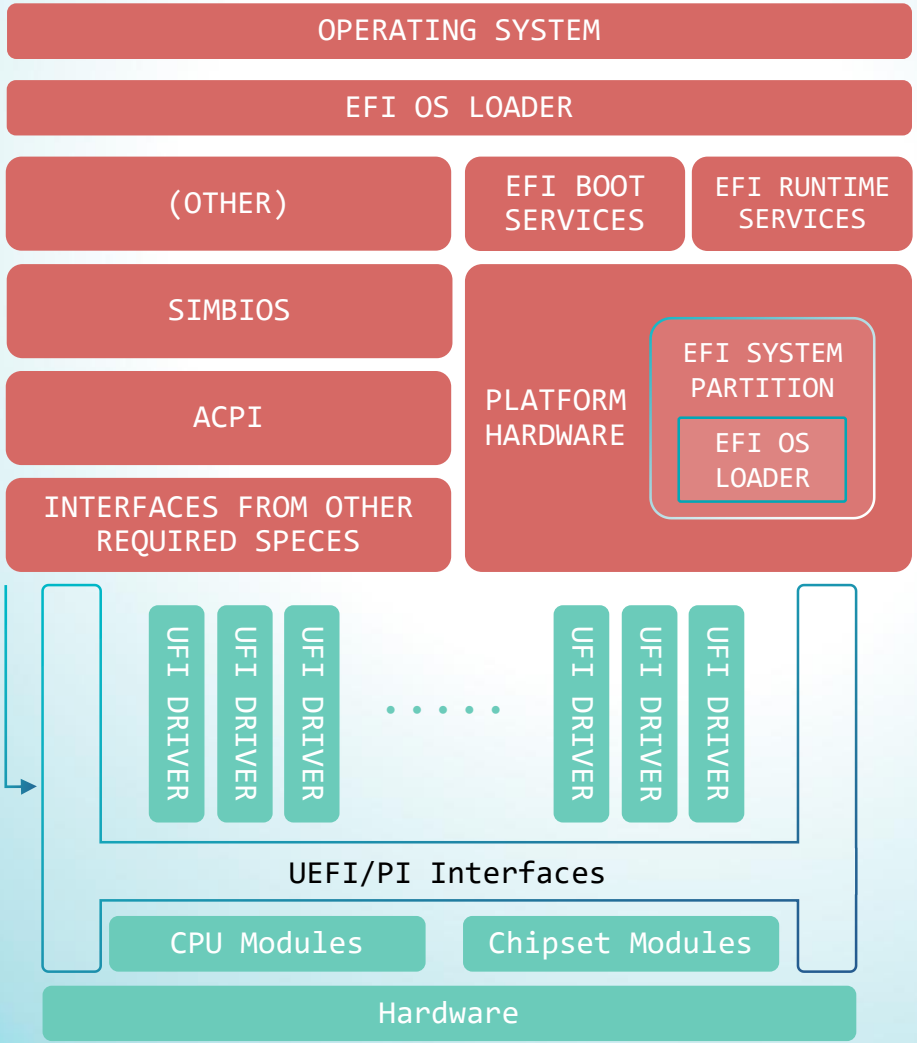
Все средства защиты установленные в ОС бессильны если:

- Любой пользователь может включить компьютер
- Получить доступ к UEFI BIOS
- Загрузить любую ОС с внешнего носителя

Доверенная загрузка – «Старая школа»

Цель безопасности	• Защита от внутренних нарушителей
Механизмы защиты	• Идентификация и аутентификация • Контроль целостности программной среды • Передача управления доверенному загрузчику
Исполнение	• Аппаратно-программное





Всё развивается и меняется

- На смену Legacy BIOS пришёл UEFI BIOS
- UEFI BIOS – «небольшая ОС»
- В UEFI BIOS можно загружать и выполнять произвольный код

Доверенная загрузка – «Новая школа»

Цель безопасности	• Защита от внутренних нарушителей • Защита от внешних нарушителей • Защита платформы от стороннего воздействия в процессе «цепочки поставки»
Механизмы защиты	• Идентификация и аутентификация • Контроль целостности программной среды • Передача управления доверенному загрузчику и контроль SecureBoot • Защита UEFI BIOS от попадания стороннего кода • Контроль и блокировка специфичных для UEFI объектов (NVRAM-переменные, ACPI-таблиц WPBT, Контроль программных SMI, прямая запись на HDD из BIOS)
Исполнение	• Аппаратно-программное • Программное

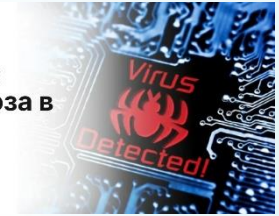
Вопрос

Что повлияло на увеличение ключевых задач и механизмов защиты модулей доверенной загрузки?

Уязвимости и зловреды

MosaicRegressor:
Lurking in the
Shadows of UEFI

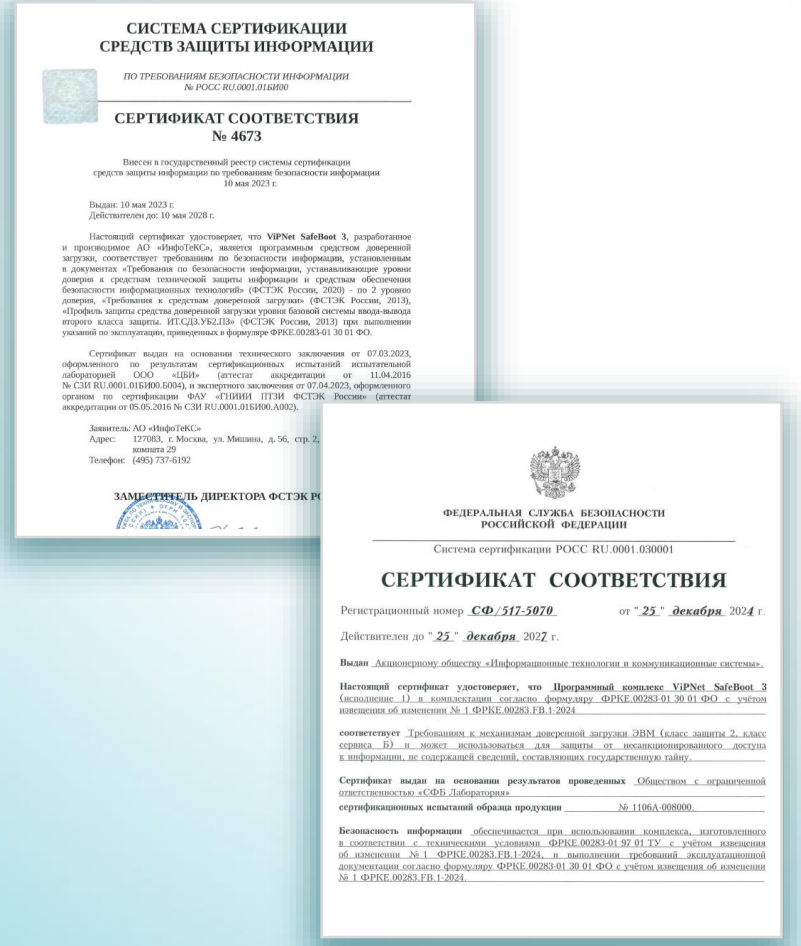
MoonBounce:
скрытая угроза в
UEFI
#новости



Мы знаем как решить проблему доверенной загрузки и защиту UEFI BIOS

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.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4673

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
10 мая 2023 г.

Выдан: 10 мая 2023 г.
Действителен до: 10 мая 2028 г.

Настоящий сертификат удостоверяет, что **ViPNet SafeBoot 3**, разработанное и производимое АО «ИнфоТеКС», является программным средством доверенной загрузки, 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 2 уровню доверия, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00283-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 07.03.2023, оформленного по результатам сертификационных испытаний испытателей лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 07.04.2023, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК Р

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/517-5070* от "*25*" *декабря* 2024 г.

Действителен до "*25*" *декабря* 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс ViPNet SafeBoot 3 (исполнение 1) в комплектации согласно формуляру ФРКЕ.00283-01 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024

соответствует Требованиям к механизмам доверенной загрузки ЭВМ (класс защиты 2, класс сервиса Б) и может использоваться для защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»
сертификационных испытаний образца продукции № 1106А-008000.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00283-01 97 01 ТУ с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00283-01 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00283.ГВ.1-2024.

ViPNet SafeBoot 3

Первые! кто получил (второй раз подряд) два сертификата на одну версию!

- ФСТЭК России № 4673
- ФСБ России № СФ/517-5070 (срок действия положительного заключения 10 лет, сертификата 3 года)

Напомним про «новые» требования

Новые требования

Средства защиты информации реализующие механизмы доверенной загрузки II класса, тип сервиса Б.

Расшифровываем:

II класс – предназначен для защиты информации ограниченного доступа (без ГТ)

Тип сервиса Б – без возможностей удалённого управления

ViPNet SafeBoot 3 может быть поставлен в двух исполнениях

Исполнение 1

- Сертифицировано в ФСБ России и ФСТЭК России
- Ввиду ограничений накладываемых сертификатом ФСБ в исполнении 1 имеются ограничения:
  - Отсутствуют «сетевые» возможности (загрузка ОС по сети, удалённое управление, аутентификация на LDAP\AD)
  - Пароль для пользователя задаётся только при помощи ПДСЧ
  - Отсутствует возможность использования на ARM

Исполнение 2

- Сертифицировано в ФСТЭК России
- Функциональных ограничений нет!

Возможности ViPNet SafeBoot 3

Идентификация и аутентификация

- Варианты идентификации и аутентификации:
  - Логин + пароль
  - Логин + сертификат на токене
  - Логин + сертификат на токене + пароль
  - Логин + PIN на токене
- Возможность идентификации и аутентификации на LDAP/AD (используются доменные учётные записи)
- Реализация SSO с ViPNet SafePoint и операционными системами

Поддерживаемые идентификаторы

- Рутокен ЭЦП
- Рутокен ЭЦП 2.0 2000, 2100, 4000
- Рутокен Lite 1000
- Рутокен ЭЦП PKI 1800
- Рутокен S 1100
- Рутокен ЭЦП 3.0 3100, 3220
- ФОРОС ST23L80
- ФОРОС ST23R160
- ФОРОС ST31H320
- ESMART Token ГОСТ с разметкой 2.2

- JaCarta LT
- JaCarta PKI
- JaCarta-2 ГОСТ
- JaCarta PKI/ГОСТ
- JaCarta-2 PKI/ГОСТ
- JaCarta-2 SE
- JaCarta PRO
- Guardant ID
- Guardant ID версии 2

Контроль целостности программных и аппаратных компонентов

- файлов на диске (на разделах с ФС FAT*, NTFS, ext2/3/4)
- реестра Windows (на уровне ключей/значений)
- CMOS (на уровне регистров)
- конфигурационных пространств PCI
- таблиц ACPI
- структур SMBIOS (DMI)
- карты распределения памяти
- модулей UEFI BIOS
- загрузочных секторов диска (загрузочного)
- переменных NVRAM
- системных таблиц UEFI

Режимы загрузки ОС

- Использование параметров загрузки BIOS
- Режим совместимости (Legacy – для «старых» платформ)
- UEFI- загрузка, передача управления загрузчику напрямую
- Загрузка ОС по сети (PXE-boot и HTTP-boot)

Дополнительные функции безопасности

- Защита UEFI BIOS
  - Защиту BIOS от записи и чтения
  - Защита после S3 - защита при выходе из спящего режима
  - Блокировка обновлений UEFI BIOS
  - Фильтрация и контроль программных SMI
- Защита от malware
  - Блокировка ACPI WPBT
  - Защита дисков от записи
  - Блокировка UEFI Option Rom
- Эмуляция NVRAM (защита от записи и чтения EFI-переменных)

Итого - общая схема работы

Финальный этап доверенной загрузки

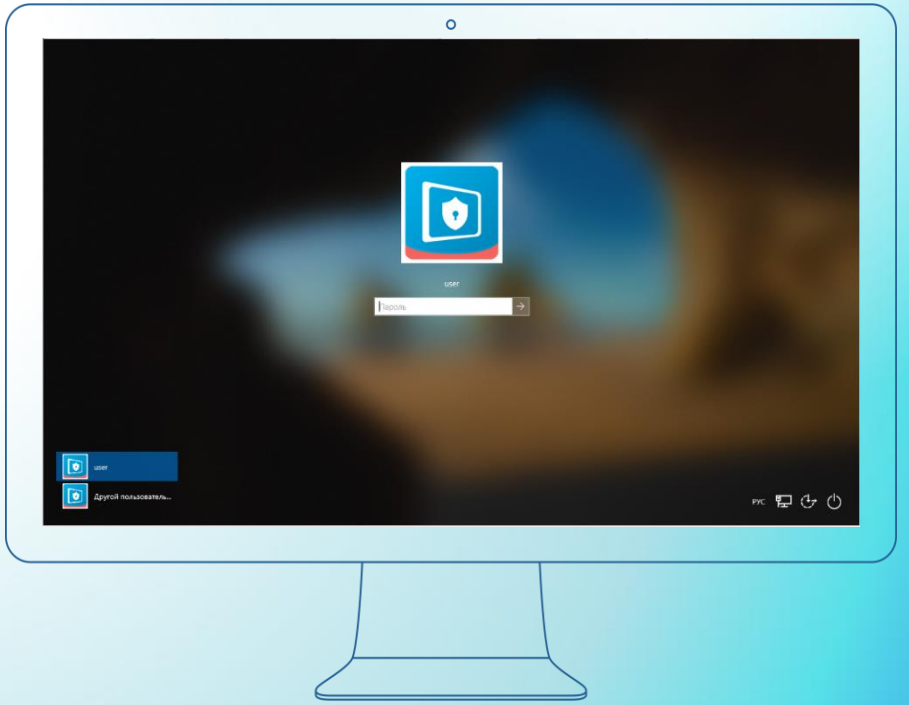
ТЕХНО infotecs ФЕСТ

ViPNet SafeBoot 3 передаёт управление загрузчику операционной системы (не используя SecureBoot).

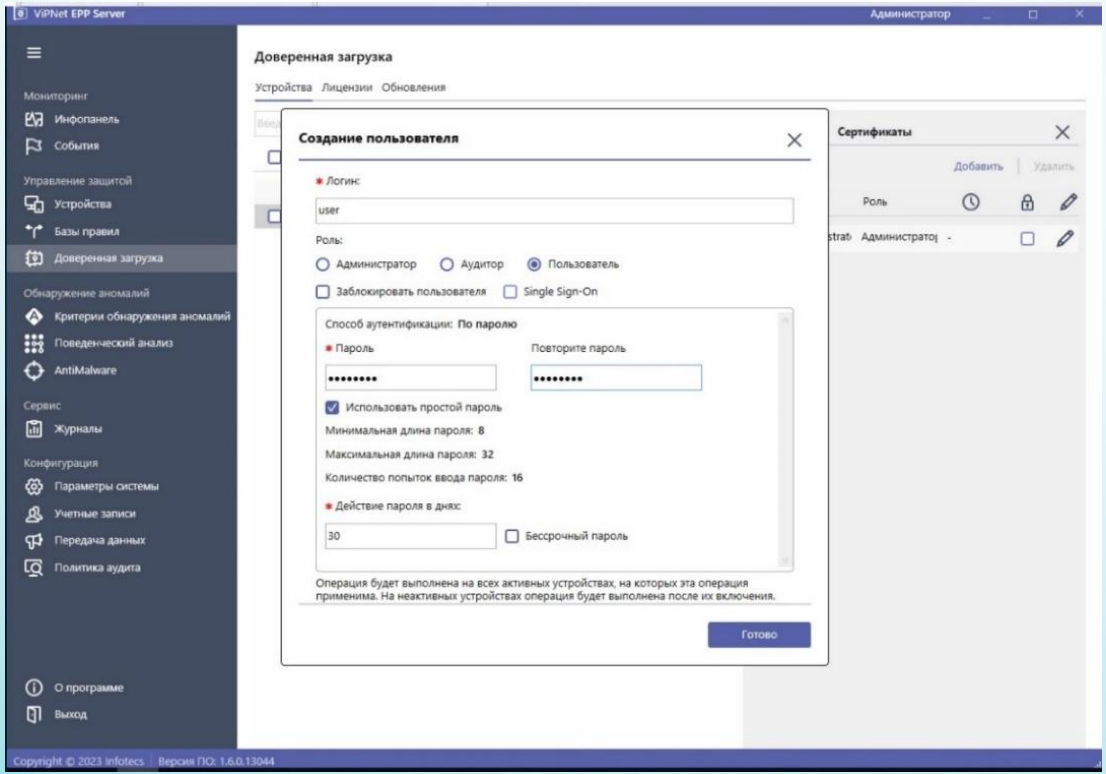
Операционная система должна быть:

- Сертифицированной
- Несертифицированной, с наложенными СЗИ от НСД

Для удобства использования есть механизм SSO – передача аутентификационных данных в ОС или ViPNet SafePoint



Управление ViPNet SafeBoot из ViPNet EndPoint Protection



Механизмы удалённого управления ViPNet SafeBoot:

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

ViPNet SafeBoot 3 и поддержка ARM

В новом релизе – поддержка ARM

Да! Мы знаем, как это сделать!
Да! У нас получилось!

- Для встраивания нашего МДЗ необходимо UEFI окружение, которое можно реализовать на платформах ARM с EDK II
- Такое окружение можно делать, как совместно с производителями «железа», так и собственноручно

Исполняемое окружение UEFI: firmware edk2

Применяемый подход в контексте текущей специфики ARM:

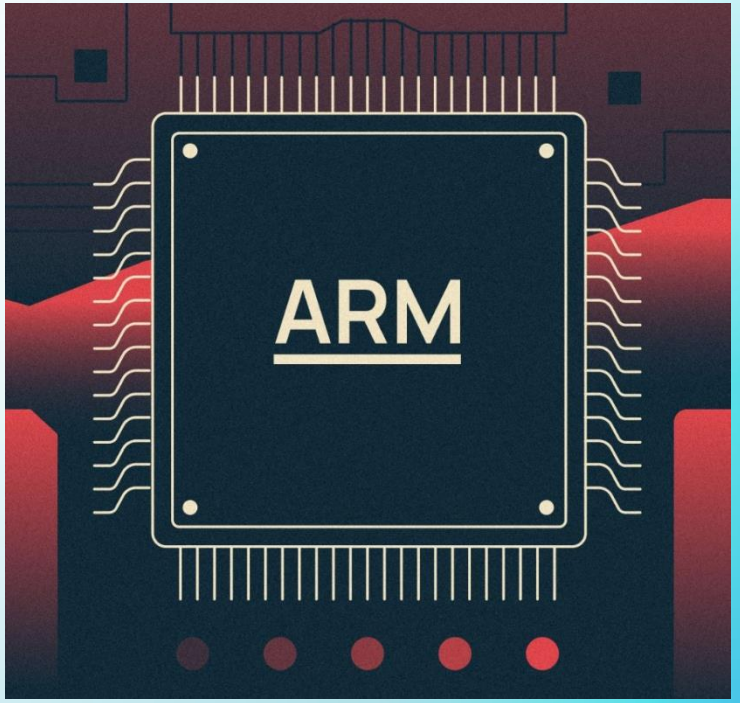
- получение исходного кода firmware edk2
- адаптация firmware edk2 (и, возможно, более ранних стадий цепочки firmware)
- установка (миграция с альтернативных типов firmware) и базовые проверки адаптированной версии firmware edk2
- реализация внешнего модуля защиты firmware
- установка ViPNet SafeBoot и внешнего модуля защиты (средствами инсталлятора или при сборке firmware)

Уже проделанный путь

В рамках работ по релизу 3.2.1 подготовлено окружение для следующих ARM-платформ, построенных на чипах:

- Broadcom 2711/2837 (Raspberry Pi 3/4/400)
- RockChip 3566/3568 (Orange PI 3B, Firefly ROC-RK3566-PC, Firefly ROC-RK3568-PC, ПАК HW10 F1)

В данный момент мы активно работаем с нашими технологическими партнёрами по данному направлению – следите за новостями



ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA
NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ
GLOBAL DIGITAL SPACE
CISOCLUB
РУТОКЕН
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
АВАНГАРД
AR integ
АТБ ЭЛЕКТРОНИКА
infotecs {/-cademy}
merlion
УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС