РЕД ОС. Операционная система как основа защиты КИИ

Докладчик: Ивлев И.В.

Заместитель директора департамента развития системных продуктов

РЕДСОФТ

Москва, 2019

О Компании

- **РЕД СОФТ** - российский поставщик решений на основе программного обеспечения с открытым исходным кодом
- Разработка, внедрение и сопровождение **прикладного и общесистемного программного обеспечения** в Российской Федерации
- Общая численность сотрудников: **более 170 человек**
- Подразделения: **Москва, Дубна, Муром, Тверь**
- Лицензиат **ФСТЭК России, ФСБ России**
- Член **АРПП «Отечественный софт»**
- Резидент **инновационного центра "Сколково"**

АРПП Отечественный софт

Sk Технопарк

Операционная система РЕД ОС

- Linux-совместимый дистрибутив на основе RPM-формата пакетной базы
- Разрабатывается с **2014** года
- Права принадлежат российской компании РЕД СОФТ
- **Зарегистрирована** в Едином реестре российских программ для ЭВМ и баз данных Минкомсвязи России (№3751)
- Сертифицирована в системе **ФСТЭК России**

Общие сведения о РЕД ОС

- **Ядро 4.19**
- Включает в себя более **25 000 пакетов**
- **Две редакции**:
  - «Стандартная» - наиболее свежий и актуальный набор пакетов
  - «Сертифицированная» - сертифицирована ФСТЭК России
- **Две конфигурации**:
  - «Сервер»
  - «Рабочая станция»

Сертификация по требованиям безопасности информации

- сертификат **ФСТЭК России №4060 от 12.01.2019 г.**
- Профиль защиты **ИТ.ОС.А4.ПЗ.**
- РЕД ОС может применяться:
  - **ГИС** до **первого класса** включительно
  - **ИСПДн** до **первого уровня** включительно
  - **КИИ** до **первой категории значимости** включительно
- **регулярный** инспекционный контроль

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4060

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
12 января 2019 г.

Выдан: 12 января 2019 г.
Действителен до: 12 января 2024 г.

Настоящий сертификат удостоверяет, что **операционная система «РЕД ОС»**, разработанная и производимая ООО «РЕД СОФТ» в соответствии с техническими условиями ТУ 02.01-001-29926343-2017, является операционной системой, соответствует требованиям по безопасности информации, установленным в документах «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016) и «Профиль защиты операционных систем типа А четвертого класса защиты. ИТ.ОС.А4.ПЗ» (ФСТЭК России, 2017) при выполнении указаний по эксплуатации, приведенных в формуляре RU.29926343.02.01-01 30.

Сертификат выдан на основании технического заключения от 02.11.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией ЗАО ГИЦ ПС ВТ (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.Б005), и экспертного заключения от 26.11.2018, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: ООО «РЕД СОФТ»
Адрес: 105066, г. Москва, ул. Доброслободская, д. 6 стр. 1, эт. 4, пом. I, ком. 7
Телефон: (495) 285-6268

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Основная нормативная база КИИ

- **187-ФЗ от 26.07.2017 г.** «О безопасности критической информационной инфраструктуры Российской Федерации»
- **ПП РФ №127 от 08.02.2018 г.** «Об утверждении Правил категорирования объектов КИИ…»
- **Приказ ФСТЭК России № 235 от 21.12.2017 г.** «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ…»
- **Приказ ФСТЭК России № 239 от 25.12.2017 г.** «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ…»

Некоторые ключевые моменты защиты КИИ

- **Реализация мер по обеспечению безопасности** для значимого объекта соответствующей категории значимости
- Применение **сертифицированных СЗИ**
- Обеспечение **непрерывного функционирования КИИ** (отказоустойчивость)
- Обязательная **техническая поддержка СЗИ**
- **Обновления** информационной безопасности
- Эксплуатация СЗИ **в соответствии с документацией** на средство

РЕДСОФТ

РЕД ОС может применяться для защиты КИИ

Приказ ФСТЭК России № 239 от 25.12.2017 г.:

28. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Категория значимости объекта КИИ	Уровень контроля отсутствия НДВ	Класс защиты СЗИ
1 категория	Не ниже 4 уровня	Не ниже 4 класса
2 категория	Не ниже 4 уровня	Не ниже 5 класса
3 категория	—	Не ниже 6 класса

Профиль защиты операционных систем ИТ.ОС.А4.ПЗ включает:

- Контроль отсутствия НДВ по 4 уровню
- 4 класс защиты СЗИ

РЕДСОФТ

10 из 17 базовых наборов мер реализуются РЕД ОС

Требования к мерам защиты

- I. Идентификация и аутентификация (ИАФ)
- II. Управление доступом (УПД)
- III. Ограничение программной среды (ОПС)
- IV. Защита машинных носителей информации (ЗНИ)
- V. Аудит безопасности (АУД)
- VI. Антивирусная защита (АВЗ)
- VII. Предотвращение вторжений (компьютерных атак) (СОВ)
- VIII. Обеспечение целостности (ОЦЛ)
- IX. Обеспечение доступности (ОДТ)
- X. Защита технических средств и систем (ЗТС)
- XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- XII. Реагирование на компьютерные инциденты (ИНЦ)
- XIII. Управление конфигурацией (УКФ)
- XIV. Управление обновлениями программного обеспечения (ОПО)
- XV. Планирование мероприятий по обеспечению безопасности (ПЛН)
- XVI. Обеспечение действий в нештатных ситуациях (ДНС)
- XVII. Информирование и обучение персонала (ИПО)

Мера реализуется средствами ОС
Мера реализуется навесными СЗИ
Организационная мера

РЕДСОФТ

Как реализовать оставшиеся наборы мер на РЕД ОС?

VI. Антивирусная защита (АВЗ)

VII. Предотвращение вторжений (компьютерных атак) (СОВ)

XII. Реагирование на компьютерные инциденты (ИНЦ)

KASPERSKY lab

STAFFCOP

POSITIVE TECHNOLOGIES

MAXPATROL™

РЕДСОФТ

Дополнительные компоненты системы защиты КИИ

КРИПТОПРО

Аладдин рд

infotecs®

ZECURION

КОД БЕЗОПАСНОСТИ

ОКБ АП

компания АКТИВ

РЕДСОФТ

Предлагаемое типовое решение защиты КИИ на базе РЕД ОС

ПК VipNET Client 4.5.3

СКЗИ КриптоПРО CSP 4.0

MaxPatrol SIEM Agent/Scanner

АВЗ Kaspersky Endpoint Security 10.1.1 для Linux

Операционная система РЕД ОС

СПО СЗИ Аккорд-Х К

ПАК Jacarta PKI/ГОСТ

РЕДСОФТ

Единый реестр российских программ

Офисное программное обеспечение

МойОфис, Р7-ОФИС, Цирконий, CommuniGate Pro

Система удаленного мониторинга

ассистент

Системы электронного документооборота

ТЕЗИС, TESSA, CompanyMedia, ЭОС

Справочно-правовые системы

КонсультантПлюс, Гарант, КОДЕКС

Средства защиты информации

КОД БЕЗОПАСНОСТИ, КРИПТОПРО, Аладдин рд, infotecs

Система коммуникаций

TrueConf, VIDEOMOST.com video conferencing server

Специализированное ПО для медицины

ДОКА+, smart delta systems

Интернет - браузеры

Спутник, Яндекс

Специализированное ПО для госсектора

МЕГАР, РуСофт 21, БФТ IBS

Аппаратное обеспечение

TONK, AQUARIUS, kraftway, DEPO [computers], ICL ТЕХНО

Антивирусное ПО

Dr.WEB®, kaspersky

Опции расширения технической поддержки для КИИ

- Расширенное время приёма обращений вплоть до 24x7x365
- Расширение репозитория и приоритетность обновлений ИБ
- Сокращение времени реакции на обращение
- Выделенные инженеры линии технической поддержки
- Анализ происшествий
- Консультации специалистов ИБ и их участие в проектировании систем
- Оценка соответствия ОС требованиям по ИБ под нужды Заказчика
- Организация собственного жизненного цикла ОС
- Участие заказчика в формировании требований к ОС
- Формирование репозитория по требованиям Заказчика

Приглашаем к сотрудничеству

www.red-soft.ru
redos@red-soft.ru