

***Особенности реализации, опыт внедрения
отечественных решений, используемых компаниями.
Возможность соответствия требованиям бизнеса и
нормативных документов***

Киселев А.В. директор по ИБ АО «НРК-Р.О.С.Т.»





Немного теории → импортозамещение согласно законодательству

Средств защиты

Указ 250

Субъекты КИИ (все НФО)

6. Установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия,

Распоряжение Правительства РФ от 05.03.2022 N 430-р

Программного обеспечения

Указ 166

30 КИИ

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

FW

VPN 2FA

IDS/IPS

DLP

AAA

AV

SIEM

...



Целью обеспечения информационной безопасности в Компании является предотвращение нанесения Компании и ее клиентам материального, репутационного и иных видов ущерба, вследствие реализации угроз нарушения безопасности информации



Сертификат Регистрации

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - ISO/IEC 27001:2013

Настоящим удостоверяется, что: Акционерное общество «Независимая регистраторская компания Р.О.С.Т.»
ул. Стромынка, д. 18, корп. 5Б, пом. IX
Москва
107076
Россия

Выдан Сертификат №: **IS 744619**

о соответствии действующей Системы Менеджмента Информационной Безопасности требованиям стандарта - ISO/IEC 27001:2013 в отношении следующих видов деятельности:

Процессы, связанные с ведением реестра именных эмиссионных ценных бумаг, организацией и проведением общих собраний акционеров и выплатой доходов по ценным бумагам в соответствии с Положением о применимости средств управления информационной безопасности от 28,07,2021 г.

От имени и по поручению BSI:

Andrew Launn, EMEA Systems Certification Director

Дата первоначальной регистрации: 2021-09-06
Дата последней выдачи: 2021-09-06

Действителен с: 2021-09-06
Действителен до: 2024-09-05



...making excellence a habit™



СЕРТИФИКАТ



соответствия системы менеджмента требованиям стандарта ISO/IEC 27001:2013

В соответствии с процедурами TÜV AUSTRIA CERT настоящим подтверждается, что

Акционерное общество
«Независимая регистраторская компания Р.О.С.Т.»
ул. Стромынка, д.18, корп. 5Б, пом. IX
г. Москва, 107996
Российская Федерация

Применяет систему менеджмента, соответствующую вышеназванному стандарту в следующих областях:

Разработка и оказание услуг по: ведению реестра владельцев именных эмиссионных ценных бумаг, организации и проведению общих собраний акционеров, выплате доходов по ценным бумагам.

Действующее заявление о применимости: утверждено приказом №2022/ОД-04-152 от 08.04.2022

Регистрационный номер сертификата: TA420223015376

Дата первичной сертификации: 2022-12-13

Действителен до: 2026-12-12

Орган по сертификации
TÜV AUSTRIA CERT GMBH

Фильдшертафт: 2022-12-13

Данная сертификация была проведена в соответствии с процедурами аудиторирования и сертификации TÜV AUSTRIA CERT GMBH и подлежит регулярным надзорным аудитам.
TÜV AUSTRIA CERT GMBH - Deutschstraße 10 A-1230 Wien www.tuv.at

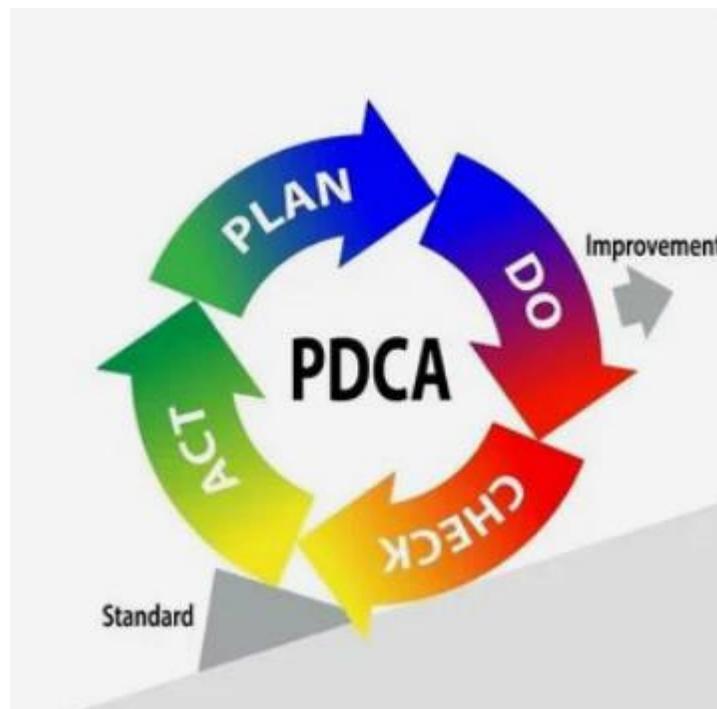


ЗЕРТИФИКАТ | CERTIFICATE | CERTIFICADO | CERTIFICAT | 証明書 | 인증서

ISO 27001

Риск ориентированный подход.

- Постоянное улучшение защищенности
(Двигатель PDCA/ISO 27001)



До 2022 **обосновано** выбрано решение которое обеспечивает требуемый уровень защищенности.

Бизнес произвел первоначальные затраты (покупка ПО, железа, затраты на внедрение, обучение персонала).

Эксплуатационные затраты.

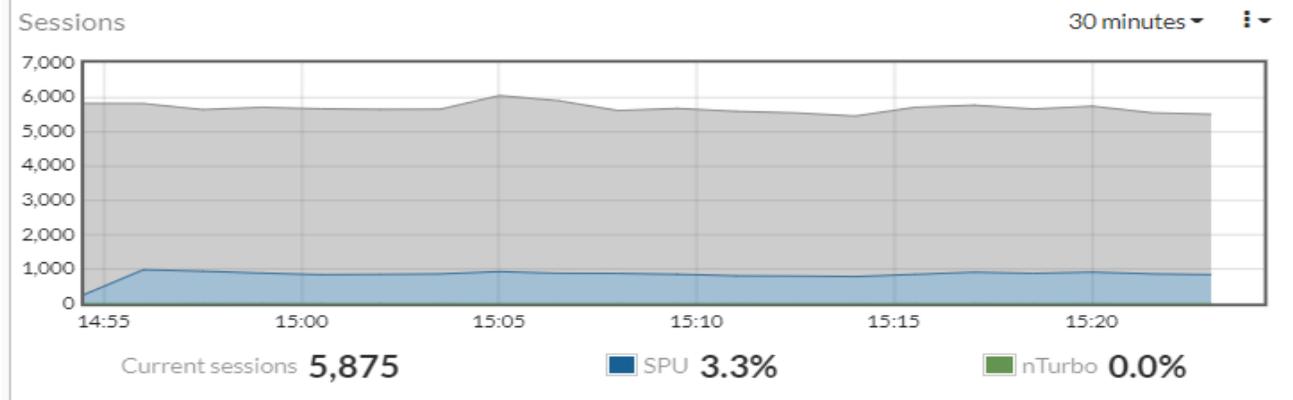
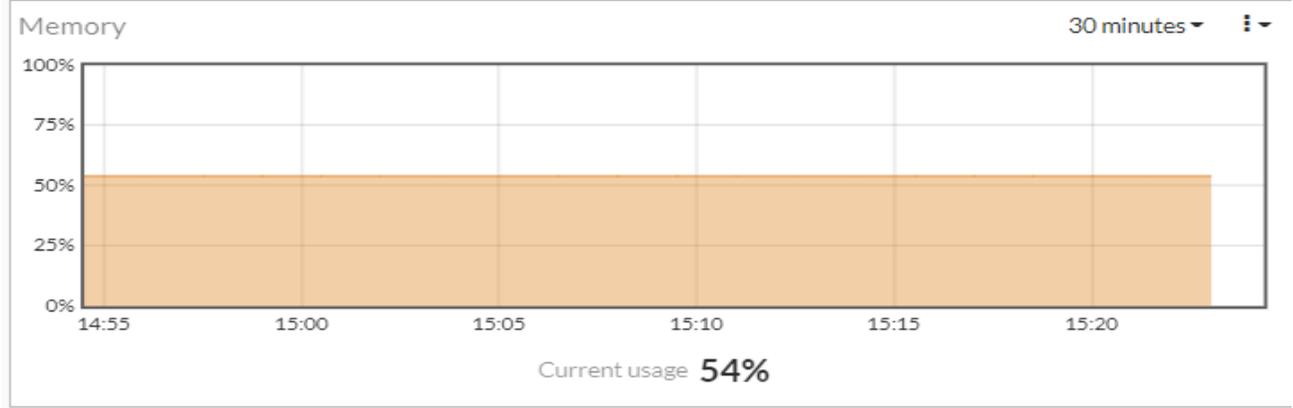
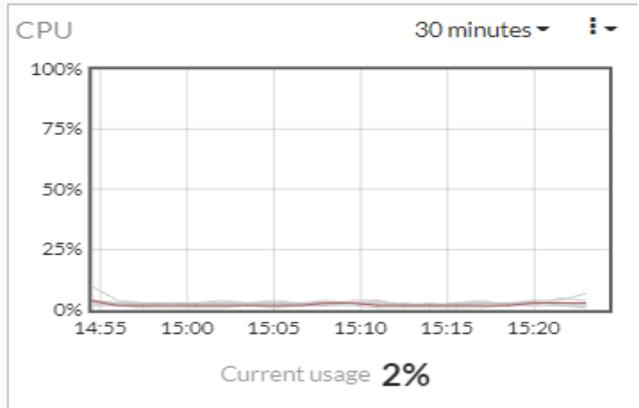
Какие проблемы мы получаем при вынужденном переходе на отечественные решения с точки зрения бизнеса:

- Затраты на тестирование решения. Риск снижения уровня защиты и качества.
- Затраты на покупку.
- Обучение и возможно поиск персонала.
- Потеря ранее вложенных средств.

Fortigate	→ UserGate
Куплено оборудование в 2019	Куплено ПО в 2022
Отсутствие официальной тех. поддержки.	Хорошая техническая поддержка.
Невозможно официально купить продукт и подписки.	Продукт развивается.
Есть клиенты под разные ОС.	Отсутствие клиентов для пользователя для ВПН (есть для 7 версии, мы пока не пробовали). Не получилось разделить права у клиентов ВПН.
Есть продуманная аналитика и дашборды.	Есть дашборды, не развитые отчеты по пользователям.
Надежность работы.	Возможность включить в кластере.

HA Status

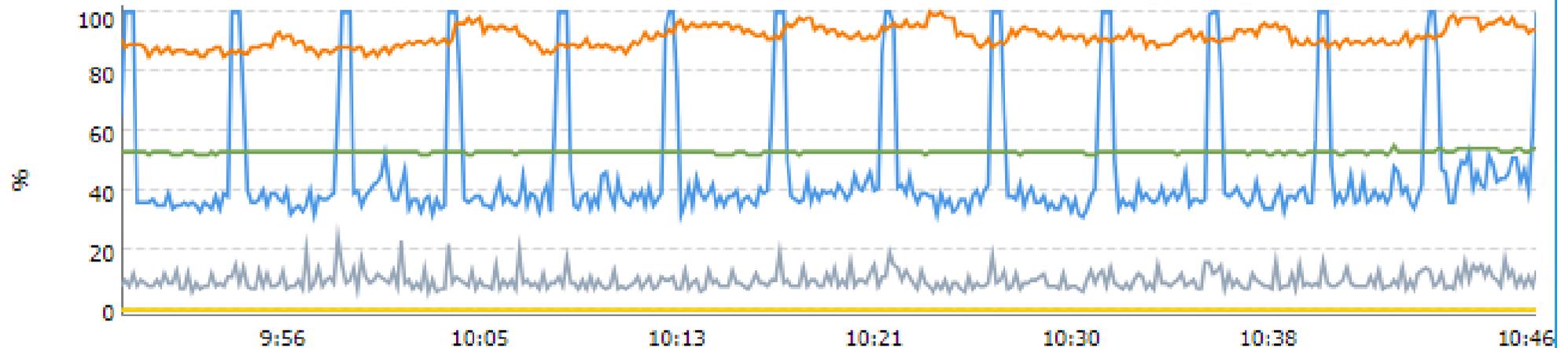
Mode	Active-Passive
Group	Main-Cluster
Primary	✔ fortiproxy
Secondary	✔ FortiROST-Spare
Uptime	1169:18:44:05
State Changed	255:15:03:18



Железо - 4 ядра хеон, 32 Гб

Графики производительности

Год | Месяц | Неделя | День | Сейчас | ↺ ×



- 10:49:41
- **Использование процессора: 100%**
 - Занятая память: 8,17 Гб из 15,27 Гб (54%)
 - Swap: 1,01 Мб из 4,00 Гб (0%)
 - Пользователи: 160 из 171 (94%)
 - vCPU: 52 из 400 (13%)

i **Внимание!**

Лицензионные ключи версий 6 и 7 несовместимы! Перед обновлением до версии 7, необходимо запросить у менеджера ключ для 7й версии.

Обновление с предыдущих версий

Обновление с более ранних версий (5, 6) не предусмотрено. Для обновления необходимо произвести экспорт настроек на внешний носитель, далее установить NGFW 7 штатными средствами, после чего импортировать ранее сохраненную конфигурацию.

i **Важно!**

Перед обновлением рекомендуется сделать резервную копию важных данных и экспорт конфигурации

ClearSwift	KSMG
Куплено в 2011	Куплено в 2022
Отсутствие официальной тех. Поддержки.	Хорошая техническая поддержка.
Невозможно официально купить продукт и подписки.	Продукт развивается.
Возможность контекстного поиска	Есть декларация, но по факту не тот функционал который нужен нам. Закрывается дополнительным продуктом.
Возможность настройки политик для маршрутизации писем.	
Удобный интерфейс.	Удобный интерфейс.
Дороже.	Дешевле.
Подключаемые антивирусные ядра.	Встроенное ядро без возможности подключения.



Контентная фильтрация сообщений

Статусы контентной фильтрации сообщений

Включение и отключение контентной фильтрации сообщений

Настройка максимального уровня вложенности архивов и контентной фильтрации

Настройка стандартных значений параметров модуля контентной фильтрации

Контентная фильтрация сообщений

Kaspersky Secure Mail Gateway выполняет контентную фильтрацию сообщений, проходящих через почтовый сервер. Вы можете ограничить пересылку почтовым сервером сообщений с определенными параметрами.

Контентная фильтрация сообщений производится по одному из следующих параметров:

- размеру сообщения;
- маскам имен вложенных файлов;
- форматам вложенных файлов.



Вы можете [указать максимальный размер сообщения с вложением, задать маски нежелательных имен вложенных файлов и указать нежелательные форматы вложенных файлов.](#)

Круговорот сканеров в Компании.



Что было до 2022 года.

Что стало после.

Что будет после 2024?

Выводы найти замену СЗИ из недружественных стран → возможно.

Необходимо иметь протестированный запасной вариант.

В некоторых случаях вместо одного решения приходится использовать несколько.

Растут затраты (тестирование, приобретение, внедрение, эксплуатация).

С точки зрения бизнеса: переход несет затраты, нужны обоснования для принятия бизнесом решений.

СПАСИБО ЗА ВНИМАНИЕ

Директор по информационной безопасности АО «НРК-Р.О.С.Т.», АО «НРК Фондовый Рынок»

Киселев Андрей Васильевич

www.rrost.ru