Актуальные вопросы защиты ЦОД
Из опыта разработчика сертифицированных СЗИ

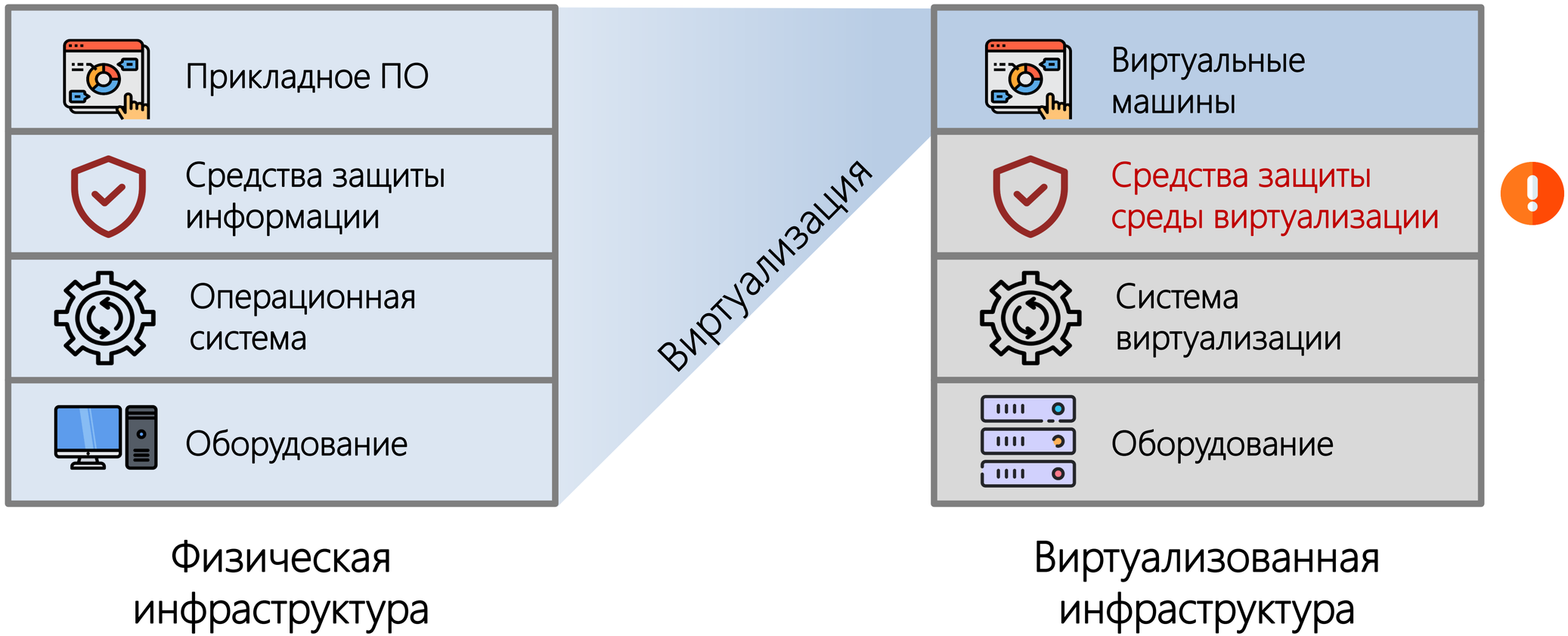
ЕВГЕНИЯ КИСЛИЦЫНА

Заместитель коммерческого директора
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Среда виртуализации



Почему сейчас?

Для защиты применяются сертифицированные СЗИ от НСД

Защита рабочих станций и серверов

Windows → Linux → Отечественные операционные системы

Для защиты применяются сертифицированные СЗИ ВИ

Защита среды виртуализации

VMware, Hyper-V → KVM, oVirt → Отечественные платформы виртуализации

Каким сертификатом должно обладать СЗИ для защиты среды виртуализации?

Защита среды виртуализации. Нормативное обеспечение

ГОСТ Р 56938—2016. Защита информации при использовании технологий виртуализации. Общие положения. (1 июня 2016 г.)

ФСТЭК России

- Приказ № 21 (ПДн)
- Приказ № 17 (ГИС)
- Приказ № 31 (АСУ ТП)
- Приказ № 239 (КИИ)

Обязательные меры **защиты среды виртуализации**, для реализации которых необходимо использовать сертифицированные СЗИ

Рекомендации в области стандартизации Банка России. **Обеспечение информационной безопасности при использовании технологии виртуализации**. (1 мая 2015 г.)

Группа мер «Защита среды виртуализации» (ЗСВ), Приказы № 17, 21 ФСТЭК России:

- **ЗСВ.1**: Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
- **ЗСВ.2**: Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
- **ЗСВ.3**: Регистрация событий безопасности в виртуальной инфраструктуре
- **ЗСВ.4**: Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

Группа мер «Защита среды виртуализации» (ЗСВ), Приказы № 17, 21 ФСТЭК России (продолжение):

- **ЗСВ.5**: Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией
- **ЗСВ.6**: Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
- **ЗСВ.7**: Контроль целостности виртуальной инфраструктуры и ее конфигураций
- …
- **ЗСВ.10**: Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

Минимальные требования к сертификации СЗИ для защиты среды виртуализации:

«Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992)

«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018)

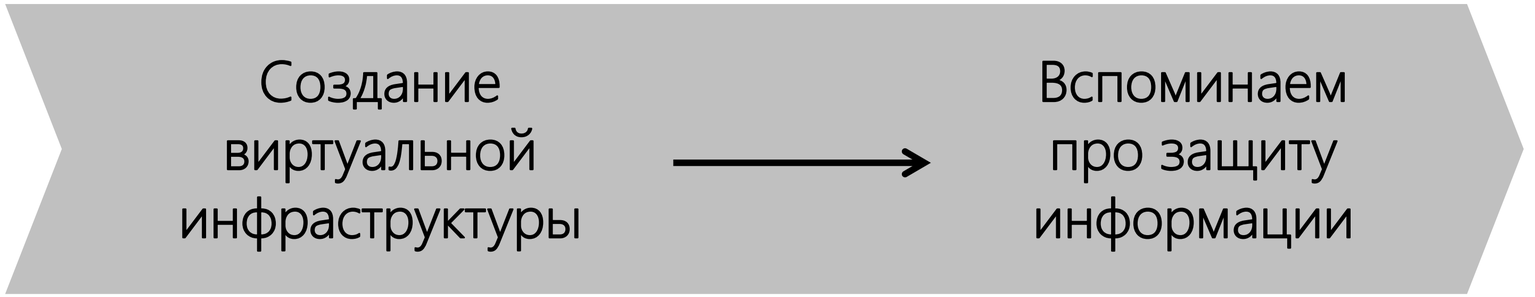
Сертифицированное СЗИ от НСД + УД

КОНФИДЕНТ®
ГРУППА КОМПАНИЙ

Тысячи проектов ежегодно реализуются в России с использованием продуктов Dallas Lock, в том числе сотни проектов по защите среды виртуализации

Особенности реализации проектов по защите ЦОД:

После создания ВИ начинают строить систему защиты и выясняется, что нужен ещё один сервер для СЗИ или лицензия на сервер виртуализации



Особенности реализации проектов по защите ЦОД:

«Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания…» — об этом почему-то иногда забывают. Нужно работать слаженно в одной команде.

Низкая квалификация кадров по виртуальным инфраструктурам и по ИБ

Практические рекомендации по основным сценариям:

«создание с нуля»

Необходимо «подружить» ИТ-специалистов по виртуальной инфраструктуре со специалистами по ИБ как можно раньше. Это позволит существенно снизить риски.

«переход с VMware»

1. *Использовать для защиты информации СЗИ ВИ с универсальными лицензиями для разнотипных гипервизоров.*
2. *При переходе на другую платформу изменяются контрольные суммы и аттестат соответствия прекращает своё действие.*

СЗИ ВИ Dallas Lock

Сертифицированная система защиты информации в виртуальных инфраструктурах. Предназначена для комплексной многофункциональной защиты конфиденциальной информации от несанкционированного доступа в виртуальных средах на базе VMware vSphere, Microsoft Hyper-V и KVM.

Продукт сертифицирован ФСТЭК России по 5 классу защищённости СВТ от НСД и по 4 уровню доверия (УД4). Сертификат ФСТЭК России № 3837 от 18.12.2017 г.

vmware®

- VMware vSphere 5.5
- VMware vSphere 6.0
- VMware vSphere 6.5
- VMware vSphere 6.7
- VMware vSphere 7.0

Microsoft Hyper-V

- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2019

KVM

- Astra Linux Common Edition «Орёл»
- Astra Linux Special Edition «Смоленск»
- CentOS 7.5.1804
- Linux Mint 18.3
- Ubuntu 18.04.2 LTS

Универсальная лицензия на СЗИ

(не требует дополнительных вложений при переходе на KVM)

Рекомендации по квалификации специалистов:

- Знание основных нормативных актов, в том числе Приказы ФСТЭК России с изложением мер защиты среды виртуализации: 17, 21. Особенно актуально для ИТ-специалистов по платформам виртуализации.
- В условиях перехода от VMware и Hyper-V на KVM-решения требуются знания в области администрирования Linux-систем и сопутствующих решений (KVM, oVirt). Подавляющее количество отечественных платформ виртуализации создаётся на базе KVM, oVirt.
- Квалификацию специалиста по продуктам Dallas Lock можно бесплатно подтвердить с помощью системы тестирования знаний на портале dallaslock.ru.

Рекомендации по квалификации специалистов (продолжение):

vmware®

- Настройка vCenter Linked Mode, VMware Auto-Deploy, vCenter High Availability, VMware Fault Tolerance

Microsoft Hyper-V

- Управление серверами Hyper-V через System Center Virtual Machine Manager
- Настройка Failover Cluster Manager

KVM

- Навыки администрирования Linux
- Сетевые технологии: OSI, Routing, Vlan, DHCP, DNS и т.п.
- Опыт работы с oVirt, Libvirt Qemu KVM
- Автоматизация задач с помощью: shell, python, ansible
- Знание аппаратной части серверного оборудования и систем хранения данных

Спасибо за внимание!

ЕВГЕНИЯ КИСЛИЦЫНА

Заместитель коммерческого директора
ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU