SAFEPHONE

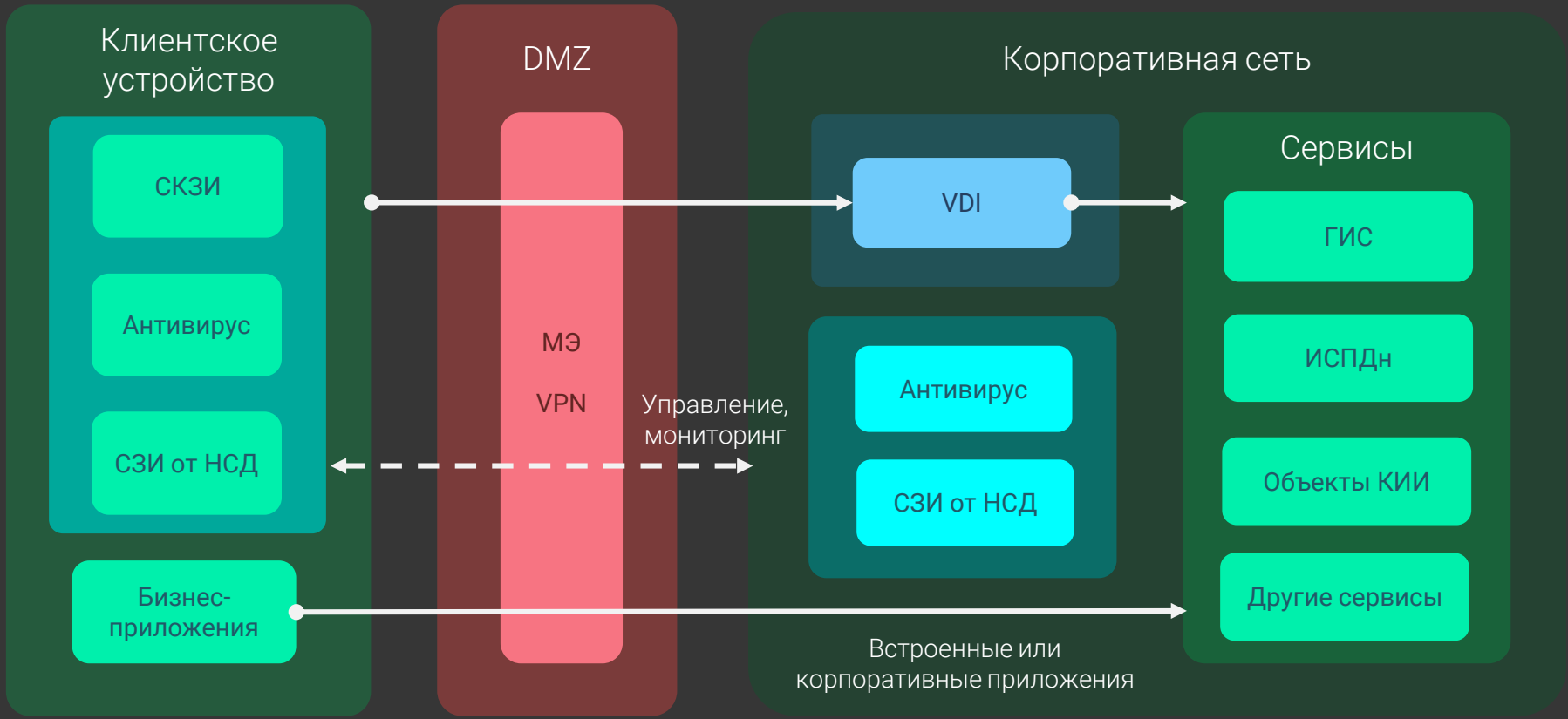
Практика защиты мобильных устройств при подготовке к аттестации объектов информатизации

НИИ СОКБ

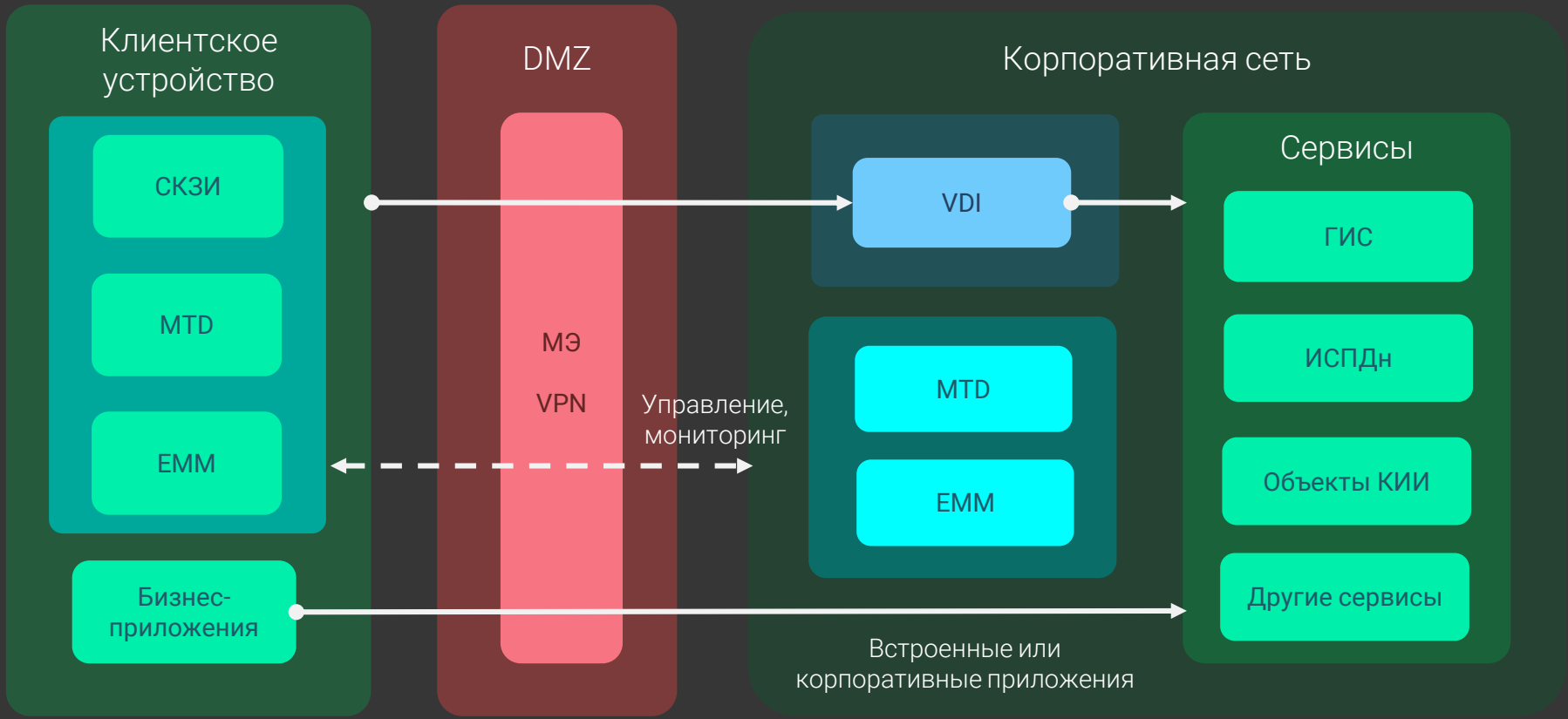
План доклада

1. Архитектура защищённого удалённого доступа
2. Выполнение требований по защите данных на мобильных устройствах в ГИС, КИИ и ИСПДн
3. Особенности защиты мобильных устройств – специфические угрозы и меры компенсации

Архитектура защищённого удалённого доступа



Архитектура защищённого удалённого мобильного доступа



Меры зашиты мобильных устройств

НИИ СОКБ

Требование	VPN	EMM	MTD
Идентификация и аутентификация (ИАФ)	Да	Да	–
Управление доступом к функциям мобильного устройства (УПД)	–	Да	–
Ограничение программной среды (ОПС)	–	Да	–
Защита машинных носителей информации (ЗНИ)	–	Да	–
Регистрация событий безопасности (РСБ)	Да	Да	Да
Анализ защищённости информации (АНЗ)	–	Да	–
Антивирусная защита (АВЗ)	–	Да	Да
Защита ИС и канала передачи данных (ЗИС)	Да	Да	–

Правила генерации и смены паролей

НИИ СОКБ

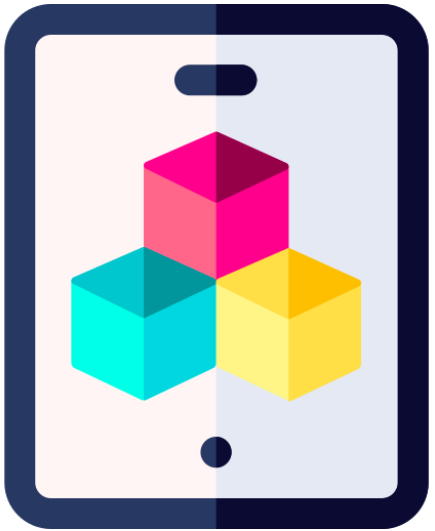
Политика безопасности	Значение	Мера
Минимальная длина пароля	от 6 до 8	ИАФ.1, ИАФ.4
Сложность пароля	Наличие букв / цифр / спецсимволов	ИАФ.4
Срок действия пароля	от 180 до 60	ИАФ.4
Минимальное число смен пароля до повтора	5	ИАФ.4
Пороговое значение неудачных попыток ввода пароля до сброса к заводским настройкам	от 10 до 4	ИАФ.4, УПД.6
Максимальное время неактивности до блокировки экрана паролем (мин)	от 15 до 5	УПД.10
Разрешить показывать пароль	Нет	ИАФ.5

Управление составом приложений

ОПС.2, АНЗ.2

1. Централизованное управление приложениями: установка, обновление, удаление, настройка
2. Режим «киоска», в котором доступно только одно или несколько приложений
3. Регистрация событий установки и удаления приложений

ОПС.3. Разрешение установки приложений только централизованно администратором EMM



Управление доступом к интерфейсам записи и передачи данных

Политика	Значение	Мера
Управление доступом к Bluetooth	Запрет	УПД.14, ЗНИ.4
Управление доступом к Wi-Fi	Белый список	УПД.14, ЗИС.20
Запрет изменения настроек VPN	Запрет	ЗИС.3
Запрет режима точки доступа	Запрет	УПД.14
Запрет трансляции экрана	Запрет	ЗНИ.4
Запрет передачи файлов по USB	Запрет	ЗНИ.4
Запрет подключения внешних носителей	Запрет	ЗНИ.6

Защита от мобильных угроз

НИИ СОКБ

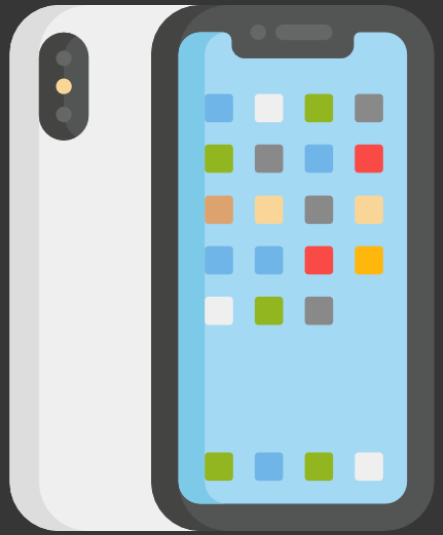
ОЦЛ.1

1. Удаление данных при обнаружении признаков программного взлома (root, jailbreak)
2. Запрет использования на устройстве режима отладки

Антивирусная защита

1. Поиск malware в приложениях и файлах на устройстве, АВЗ.1
2. Обновление локальных антивирусных баз АВЗ.2

Особенности защиты смартфонов и планшетов



Мобильное устройство просто украсть и потерять 😢

Рекомендации:

1. Блокировать доступ к потерянному устройству и искать его по данным GPS / ГЛОНАСС
2. Сбрасывать устройство к заводским настройкам*, если его не удалось найти, ЗНИ.8

   * Чтобы сброс устройства был быстрым, в процессе удаляется только AES ключ, которым зашифрованы данные

На мобильных устройствах нельзя изменить или дополнить системное шифрование 😔

Рекомендации:

1. Реализовать шифрование алгоритмами ГОСТ в приложениях, где оно необходимо
2. Использовать доверенные облачные решения для электронной подписи
3. Удалять данные при обнаружении признаков программного взлома (root, jailbreak), **ОЦЛ.1**

КИИ =

Требования ИБ

Федеральные законы № 187-ФЗ, 193-ФЗ

Приказы ФСТЭК России № 235, 236, 239 …

Импортозамещение

Преимущественное использование:

- Российского ПО **до 01.01.2023**
- Российского «железа» **до 01.01.2024**

Постановление Правительства РФ от 03.12.20 № 2013 требует покупать российские планшеты уже с января 2021

НИИ СОКБ

SAFEPHONE

Единая платформа управления

android

ASTRA LINUX®

SAFEPHONE

Спасибо за внимание!

НИИ СОКБ

Москва, Научный проезд, д. 17

www.niisokb.ru

+7 (495) 646-75-63