



Министерство цифрового развития,
связи и массовых коммуникаций
Российской Федерации

Типовое автоматизированное рабочее место государственных служащих

Директор Департамента
проектов по информатизации

Гурзов К.А.

10 февраля 2021

Предпосылки и цели создания сервиса ТАРМ

Предпосылки

1 **Отсутствие базовых российских сервисов**

28% госслужащих не имеют корпоративной почты (*)

2 **Цифровое неравенство**

Неравные доли затрат на ИТ для регионов и ФОИВов

3 **Удобство использования**

Рабочие сервисы **не должны уступать** в удобстве использования рыночным аналогам

4 **Утечки информации**

23% утечек происходят в госсекторе (**)

Цели и результаты

- Обеспечение доступности удобных рабочих базовых инструментов
- Заместить 100%** бесплатных рабочих сервисов (электронная почта, мессенджер, ВКС/АКС, файловое хранилище)

- Устранить неравенство в доступности технологий и сервисов между органами власти
- Предоставить возможность 100%** ГГС и муниципальных служащих воспользоваться платформой

- Для **повышения показателей** эффективности необходимо создать функционал внутриведомственных и межведомственных коммуникаций
- Создать сервисы и инструменты не уступающие рыночным аналогам

- Устранить **причины неисполнения** мер ИБ с сохранением комфорта использования

Задачи

- Создать централизованные базовые сервисы для всех органов власти, с едиными стандартами и протоколами
- Внедрение вовлекающих механик и инструментов
- Обеспечение сквозной интеграции коммуникативных инструментов в госсекторе

- Дать единый уровень доступности цифровых инструментов для всех ФОИВов/РОИВов/ОМСУ/ бюджетных учреждений
- Централизовать инфраструктуру для ИТ решений

- Внедрение российских инструментов
- технологии с открытым исходным кодом
- Передовые технологических партнеры
- создать функционал внутриведомственных и межведомственных коммуникаций.

- Перевод госслужащих в защищенный контур
- Повышение контроля за передачей информации
- Создать инструменты работы с ДСП

(*) - из результатам опроса Минцифры России по 64 ФОИВам, исключая множественные и вневедомственные ящики

(**) – по данным ГК InfoWatch

Базовые сервисы

По результатам опроса 64 ФОИВ Минкомсвязью России:

- **83%** используют сервисы Microsoft для организации почты
- **59%** ФОИВов не используют интеграций с коммуникационными системами
- **19%** не имеют комплементарных базовых сервисов (организация встреч, календари рабочего времени и пр.)
- Нет единого стандарта защиты и сохранности служебной информации



Необходимо обеспечить доступность удобных рабочих базовых инструментов и сервисов, на базе отечественных разработок и технологий:



Корпоративная почта

- Почта
- Рабочий календарь
- Адресная книга



Мессенджер / АКС / ВКС

Сегодня сотрудник в среднем использует **3** бесплатных облачных мессенджера в своей работе для переписки с коллегами

3 Мб служебной информации ежедневно отправляет сотрудник ведомства через незащищенные мессенджеры



Файловое хранилище

В 3 раза сокращается время на поиск и отправку файлов при использовании корпоративного файлового хранилища



Кадровые сервисы и управление развитием

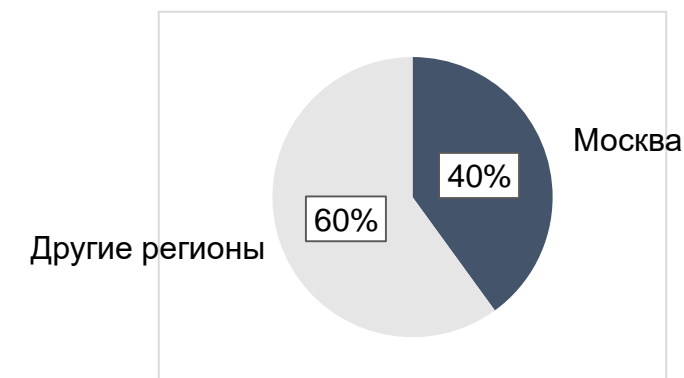
- Модуль профессиональной адаптации и ориентации
- Модуль управления знаниями
- Сервисы опросов
- Модуль планирования совещаний

Цифровое неравенство

Из отчета McKinsey «Digital Russia Report»:

- Использование передового опыта в создании цифровых продуктов в наиболее продвинутых регионах, как общий подход для цифровизации государственных органов
- Основной бюджет на ИКТ сконцентрирован на лидирующих в цифровизации регионах, что означает отставание других регионов в цифровизации, и необходимость передачи технологий и опыта этим регионам

Распределение расходов на ИТ, %



Подсистема информационной безопасности ТАРМ

Проблемы информационной безопасности



- Утечка конфиденциальных документов или их временных копий при временной передаче собственных устройств третьим лицам, их продаже, сдаче в ремонт, утере, взломе.
- Удаленная работа вне закрытого контура



- Утечка из-за преднамеренного копирования конфиденциальной информации из ведомственных информационных систем.
- Угроза взлома несертифицированных TLS устаревших версий 1.1 и 1.2 (время реализации атаки - 38 часов)



- Утечка конфиденциальной информации через онлайн-сервисы или мессенджеры при обмене и общении в рабочих группах с неконтролируемым составом участников.
- Отсутствие антивирусов

Меры пресечения

Доверенное программное обеспечение и среда исполнения (загрузка с защищённого 'токена')

Аутентификация с использованием УКЭП, «гостированная» защита обмена данными (ViPNet)

Запрет копирования загружаемых данных на не защищённые носители

Антивирусная защита, контроль целостности, контроль защищённости

Сетевая сегментация, выявление и предотвращение вторжений

Постоянный мониторинг действий и коммуникаций пользователя, фиксация событий ИБ

Типовой внутренний нарушитель (63% всех утечек (*))



рядовой сотрудник, имеющий доступ к информации ограниченного доступа в силу должностных обязанностей

не соблюдает регламент работы с ДСП, так как ознакомлен с ним формально и не считает его чем-то важным

использует собственный телефон или планшет для работы с электронной почтой и документооборотом

недоволен отношением со стороны руководства, уровнем заработной платы, отсутствием карьерного роста

использует открытые мессенджеры и онлайн-сервисы

испытывает финансовые затруднения или готов сотрудничать с внешними нарушителями за вознаграждение

ТАРМ – инструмент безопасной удалённой работы с информацией ограниченного доступа (ДСП)

- строгая аутентификация и «гостированная» защита обмена данными с использованием УКЭП;
- 100% доверенное ПО;
- мониторинг действий и коммуникаций пользователя и передаваемых данных;
- DLP позволяет выявлять и блокировать передачу чувствительной информации.

(*) – по данным ГК InfoWatch

Для всех ведомств:



- Повышение эффективности межведомственного взаимодействия, а также взаимодействия органов власти с населением
- Возможность работы из любого места, безопасная удаленная работа
- Противодействие утечкам информации
- Равноправный доступ всех ОГВ к общей витрине приложений
- Гибкая модель ценообразования: базовый набор сервисов SaaS единый для всех, остальные опции возможно дополнительно включить, в т.ч. ПО и оборудование
- Унификация технических решений, единые SLA. Информатизация ведомств в едином темпе в рамках общей «Дорожной карты»
- Возможность использования технологий TAPM для услуг бизнесу и населению



Для ведомств, **недоукомплектованных современными средствами ИТ и имеющих сложности с бюджетом:**

- Обеспечение доступности сервисов TAPM для всех сотрудников ведомства в условиях ограниченного бюджета
- Возможность работы с любого типа устройств, включая домашние ПК
- Увеличение срока использования существующего парка оборудования на 30% за счет технологии VDI
- Обеспечение передовых механизмов информационной безопасности



Для ведомств, **не имеющих проблем с бюджетом, следующим исторически сложившимся стандартам ИТ, основанных на традиционном офисном ПО:**

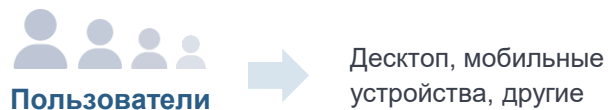
- +
- Сокращение затрат и повышение прозрачности на автоматизацию рабочих мест
- Повышение кадровой вовлеченности
- Импортзамещение коммерческих сервисов и сокращение санкционных рисков
- Повышение уровня ИБ в условиях коллективной работы с другими ведомствами за счет применения единых политик, стандартов и инструментов



Для ведомств, **активно инвестирующих в развитие внутренних и внешних ИТ сервисов и применяющих в повседневной жизни современные технологии:**

- +
- Повышение эффективности работы госслужащих за счет получения универсальных и объединенных сервисов коммуникации и коллективной работы с другими ведомствами
- Клиентский опыт: легкость и простота подключения и использования сервиса TAPM, единый интуитивно понятный интерфейс
- Возможность создания и публикации новых сервисов ФОИВ для использования другими

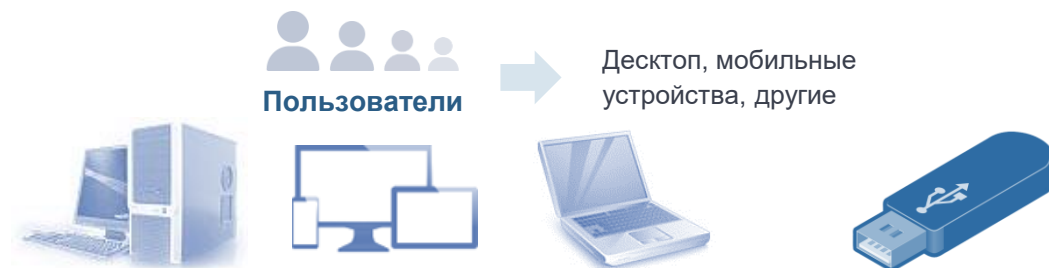
Архитектура платформы ТАРМ



ЕДИНАЯ СИСТЕМА АВТОРИЗАЦИИ
ЕСИА/LDAP

ЕИСУ КС





Live USB

Сертифицированное средство обеспечения безопасной дистанционной работы сотрудников органов исполнительной власти и государственных структур

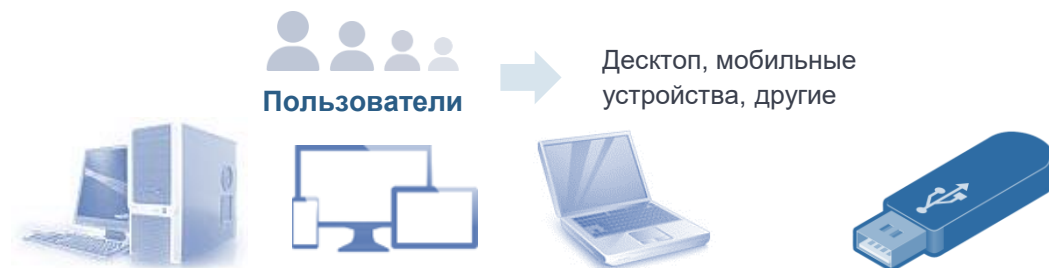
По поручению Правительства Российской Федерации совместно с ФСТЭК России и ФСБ России разработаны «Требования к устройствам обеспечения безопасной удалённой работы», дающие возможность сотрудникам органов исполнительной власти и государственных организаций удалённо работать с государственными информационными системами с применением неаттестованных средств вычислительной техники (включая личные)

Защищённое устройство должно обеспечивать:

- Загрузку компьютера с внешнего USB-носителя, на котором записана сертифицированная операционная система.
- Двухфакторную аутентификацию пользователя.
- Автоматическую настройку и подключение к шлюзу организации с использованием сертифицированного VPN.
- Удалённое подключение к рабочему столу служебного компьютера (Remote Desktop) или работу с виртуальным рабочим столом (VDI).
- Удалённый запуск и дистанционную работу с приложениями, установленными на служебном компьютере.
- Автономную работу со служебными документами с возможностью их сохранения на защищённый раздел USB-устройства.
- Хранение, формирование и проверку усиленной квалифицированной электронной подписи (УКЭП) с неизвлекаемым закрытым ключом.

Защищённое устройство должно быть сертифицировано для работы:

- В государственных информационных системах (ГИС) - до первого класса защищённости включительно
- В информационных системах персональных данных (ИСПДн) - до первого уровня защищённости включительно
- В информационных системах значимых объектов критической информационной инфраструктуры (КИИ) - до первой категории включительно
- В медицинских (МИС), банковских (ИБС) и других информационных системах (ИС) – до первого класса защищённости включительно
- В информационных системах общего пользования - II класса.



Защищённое устройство позволяет:

- Использовать личный компьютер для дистанционной или автономной работы с возможностью обработки документов ограниченного распространения.
- Использовать функции привычного USB-токена при работе со служебным компьютером:
 - для двухфакторной аутентификации при входе в ИС;
 - для электронной подписи в СЭД, ДБО, в различных электронных сервисах и Web-порталах;
 - в качестве защищённой «флешки» для хранения конфиденциальной информации.
- Отказаться от использования запоминаемых паролей, вводимых пользователями вручную, при удалённом подключении к ИС организации.
- Использовать надёжную двухфакторную аутентификацию пользователей.
- Осуществлять централизованное удалённое администрирование устройства - обновлять пользовательские настройки, профили, цифровые сертификаты, ключи доступа и т.п.

Live USB

Сертифицированное средство обеспечения безопасной дистанционной работы сотрудников органов исполнительной власти и государственных структур

Защищённое устройство предотвращает возможность:

- Использовать его на неизвестном (неавторизованном) компьютере.
- Скопировать или сохранить обрабатываемую служебную информацию на локальные, съёмные диски, флэш-накопители.
- Распечатать обрабатываемую служебную информацию на локальный или сетевой принтер.
- Загрузить на свой компьютер какой-либо файл (возможно, заражённый) с внешнего носителя или из сети Интернет и передать его в ИС организации.
- Выйти в сеть Интернет при дистанционной работе напрямую со своего личного компьютера минуя используемые в организации средства защиты.
- Получить доступ к сохранённым в памяти устройства служебным или пользовательским данным в случае утери или кражи устройства.

Удалённое рабочее место TAPM: Архитектура

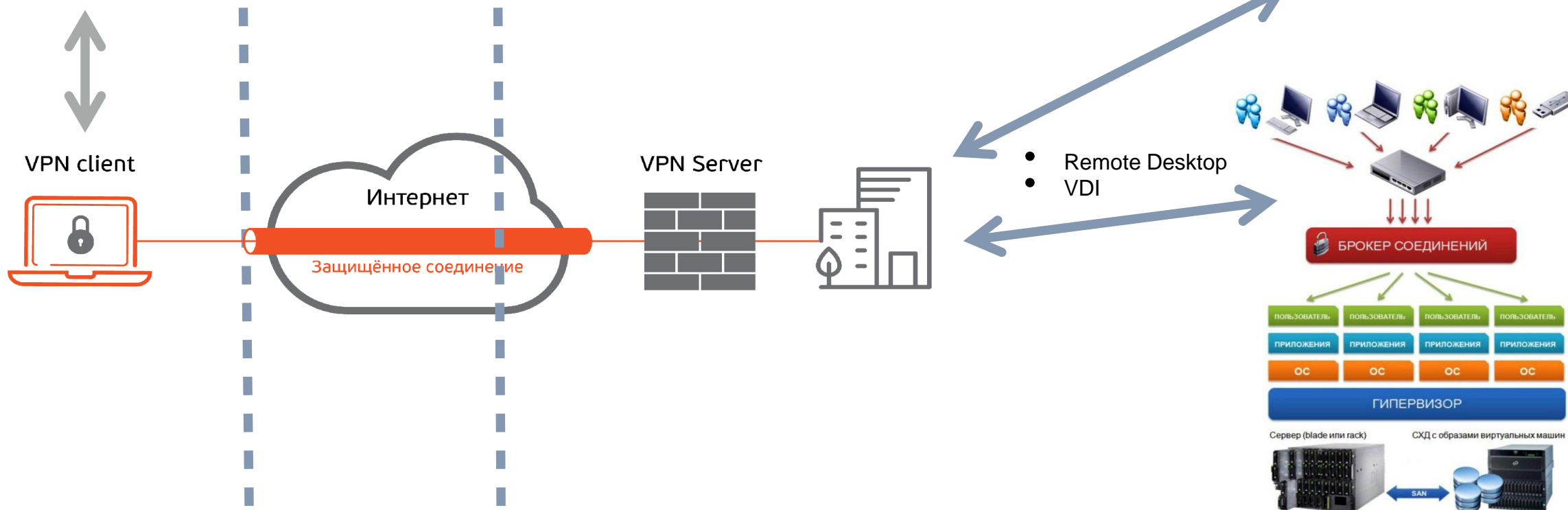
Личный ПК + Live USB



Обеспечение безопасности:

- Сертифицированные операционные системы
- Сертифицированные VPN
- Средства VDI
- Все задачи выполняются на служебном ПК или на VM, а на неаттестованный ПК передаются лишь выводимые на экран изображения

Служебный ПК



Спасибо!