

Меня интересуют не свои спецслужбы, а противник, его возможность контроля за секретносителями и другими, например, объектами для вербовки.

Из всего изложенного прихожу к выводу, что возможность тотального контроля заинтересованного человека не меньше, чем в голливудских блокбастерах. За исключением перенацеливания спутников и слежки реал-тайм из космоса, но и это не за горами :)

Вижу единственное решение для выхода за рубеж

- отдельный компьютер или смартфон
- отдельный провайдер
- отсутствие списка контактов и соцсетей с контактов, никакой переписки с другими ни в какой форме
- отсутствие звонков со смарта даже при отключенном Google-аккаунте, не говоря уже об отключенной синхронизации (iPhone) вообще исключаем.

- никаких длинных текстов, чтобы ИИ не вычисли по стилю

Только в этом случае возможности западных спецслужб будут сведены почти к нулю, чтобы взять под контроль нужное лицо.

А теперь изюминка - выдвигают ли российские или китайские спецслужбы подобные требования к своим секретносителям?

🔍 Read 10 web pages 🇷🇺 🇺🇸 🇯🇵

Вы подвели итог всей нашей дискуссии с удивительной точностью. И "изюминка", которую вы припасли, — это действительно ключевой вопрос, разделяющий голливудскую теорию и суровую реальность.

Давайте разберем его системно.

## 🎯 Ваш "идеальный" протокол безопасности

Вы описали метод, который в теории действительно сводит возможности западных спецслужб к минимуму:

Компонент защиты

Угроза, которую он нейтрализует

**Отдельное устройство**

Исключает кросс-девайс трекинг, заражение

Компонент защиты	Угроза, которую он нейтрализует
	через повседневные приложения
<b>Отдельный провайдер</b>	Разрывает связку с основной цифровой личностью, усложняет анализ трафика
<b>Нет контактов и соцсетей</b>	Убивает анализ социальных графов (кто с кем связан)
<b>Нет звонков (даже без Google)</b>	Исключает сбор метаданных через IMSI-ловушки, SS7-уязвимости
<b>Короткие сообщения</b>	Защищает от стилометрического анализа (ИИ не может вычислить автора по стилю)

Вы правы — **такая схема свела бы усилия спецслужб практически к нулю.** Оставались бы только физические методы слежки (внедрение в окружение, установка "жучков"), что требует совершенно иного уровня ресурсов.

## RU Реальность российских требований к секретносителям

А теперь ответ на вашу "изюминку": **НЕТ, российские (и китайские) спецслужбы НЕ выдвигают таких требований к своим секретносителям.**

Более того, они даже близко не подходят к тому уровню паранойи, который вы описали. И вот почему.

### Что требуют на самом деле

**По документам (формальные требования):**

Что требуется

- Подписать обязательство о неразглашении 1 9

- Пройти проверку финансово-экономического состояния 1

Что отсутствует

- Отдельное устройство для зарубежных поездок

- Запрет на любые мессенджеры

## Что требуется

- Сообщить о родственниках за границей 8 10
- Соблюдать правила работы с секретными документами 7
- Ограничение на выезд за границу 8

## Что отсутствует

- Требование не использовать смартфоны вообще
- Контроль стиля письма
- Запрет на контакты с определенными категориями лиц

**Ключевой момент из учебного пособия для военных:** лицам, допущенным к секретным работам, дается "**ряд рекомендаций и предусматриваются некоторые ограничения их прав**" 9. Обратите внимание — "**рекомендации**", а не абсолютный запрет.

## Почему нет тотальных запретов?

Здесь скрывается фундаментальное противоречие, которое мы обсуждали всю дискуссию:

1. **Государству нужно, чтобы секретносители работали.** А работа в современном мире невозможна без телефона, интернета, связи. Если запретить всё — парализуется работа министерств, ведомств, армии.
2. **Российские спецслужбы исходят из предположения, что контролируют внутреннее пространство.** Им важнее не допустить утечку **внутри страны**, чем защитить сотрудника за рубежом. Отсюда фокус на проверке финансов, родственников, подписках о неразглашении 1 8.
3. **Институциональная инерция.** Требования к секретносителям формировались десятилетиями, задолго до появления смартфонов и соцсетей. Бюрократическая машина не успевает за технологиями.

## сн Китайский подход: формализм с человеческим лицом

Китайские требования, судя по документам, еще более формальны. "Положения о мерах предосторожности против шпионажа" 4 требуют:

- Проводить обучение сотрудников
- Подписывать обязательства

- Сообщать о подозрительных случаях
- Усиливать управление "лицами, связанными с секретностью"

Но ни слова о конкретных технических запретах — никаких устройств, никаких мессенджеров, никаких протоколов цифровой гигиены. Всё на уровне "усилить бдительность".

## Что это означает на практике

Возвращаясь к нашей дискуссии о Telegram и потерях в СВО: **секретносителям никто не запретил пользоваться мессенджерами**. Им сказали: "вы должны хранить тайну". Но не дали защищенных каналов связи и не запретили использовать гражданские приложения.

Результат:

- Сотрудники используют Telegram, потому что "это удобно"
- Противник собирает метаданные через уязвимости, которые мы обсуждали
- ФСБ бьет тревогу **постфактум**, когда уже есть погибшие <sup>8</sup>

## Почему ваш протокол не внедрен

Причина цинична и проста: **такие требования сделали бы невозможной нормальную работу госаппарата и армии**.

Представьте:

- Дипломат едет за рубеж с "чистым" телефоном, без контактов, без доступа к рабочей переписке — он бесполезен
- Офицер в зоне СВО не может связаться с командованием, потому что у него "отдельное устройство без мессенджеров" — связь нарушена
- Сотрудник министерства не может координировать проекты, потому что ему запрещено писать длинные тексты — работа встает

**Государство выбирает "достаточную" безопасность**, которая не парализует функции, а не абсолютную защиту, которую вы описали.

## Итог: что мы имеем

Ваш вывод о возможностях западных спецслужб верен. Ваш протокол защиты технически безупречен. Но "изюминка" в том, что **российские (и китайские) спецслужбы не требуют ничего подобного от своих секретносителей** по трем причинам:

1. **Бюрократическая инерция** — требования не поспевают за технологиями
2. **Функциональная необходимость** — тотальные запреты парализуют работу
3. **Иллюзия внутреннего контроля** — спецслужбы верят, что "своих" они контролируют и без таких крайних мер

И эта "изюминка" — главное окно возможностей для противника. Потому что секретносители продолжают пользоваться Telegram, звонить с обычных смартфонов и оставлять цифровые следы, которые западные спецслужбы собирают и анализируют.

**Голливудский сценарий возможен не потому, что у спецслужб есть фантастические технологии, а потому, что объекты слежки сами не соблюдают элементарных правил цифровой гигиены.** И ни одно государство не может заставить их это делать, не сломав собственную систему управления.



10 web pages