ARGA

OBSERVATORY

LAWFARE AND HUMAN RIGHTS
MONITORING PLATFORM

БЛОК XII

ЦИФРОВАЯ БЕЗОПАСНОСТЬ И OSINT

www.argaobservatory.org

Связаться с нами

Общая цель раздела

Дать пошаговые правила цифровой гигиены для правозащитников, адвокатов и доверителей, которые находятся под риском преследования, утечки данных или компромата

Телефон/ноут на границе: режим «чистого въезда»

На границе ваши гаджеты = открытая книга

- Завести отдельное устройство для путешествий
- Хранить только базовые данные (без переписок, фото)
- Основное — в облаке с шифрованием

Таможня может копировать содержимое устройств. Лучший вариант — «чистый» телефон или ноутбук только для поездок

Частые ошибки:

- **ввозить с собой «основной» телефон с личной перепиской**

Legal core:

Пограничный контроль в ЕС/США имеет право на осмотр устройств

Безопасная связь с адвокатами (E2EE, метаданные)

Шифрование спасает не текст, а смысл

- Использовать Signal / ProtonMail
- VPN и TOR для маскировки
- Минимизировать время и частоту переписки

Legal core:

Международные стандарты защиты адвокатской тайны (ООН, ЕСПЧ)

Даже зашифрованный мессенджер может «сдать» метаданные (кто, когда, откуда)

Частые ошибки:

- **Думать что «безопасный чат» в WhatsApp/Telegram действительно безопасный**

OSINT-профиль доверителя: как чистить и что оставить

Ваш цифровой след — досье для врага

- Удалить старые посты, сомнительные фото
- Систематизировать упоминания в СМИ
- Создать «контролируемый» профиль (LinkedIn, сайт)

Суд, Интерпол или противники анализируют соцсети, публикации, фото. Нужно вычищать всё лишнее, оставляя только выгодное

Частые ошибки:

- **полная зачистка (подозрительно выглядит)**

Legal core:

GDPR + право на приватность (ст. 8 ЕКПЧ)

Как не «подставить» свидетелей и семью в соцсетях

Одна фотография = риск для близких

- Не выкладывать фото с геометками
- Убрать списки друзей и метки родства
- Настроить приватность

Legal core:

GDPR, право на защиту частной жизни

Публикации с родственниками или друзьями могут привести к их слежке и допросам.

Частые ошибки:

- **постить в реальном времени («мы сейчас в Париже»)**

Deepfake и фабрика компромата: как опровергать

Фейковое видео может разрушить всё — если молчать

- Собирать экспертные заключения (цифровая экспертиза)
- Сравнивать оригинальные метаданные
- Давать публичное опровержение сразу

Deepfake-компромат активно используется против оппозиции и бизнесменов

Частые ошибки:

- **замалчивать фейки или реагировать слишком поздно**

Legal core:

Практика ЕСПЧ по защите чести и репутации (ст. 8)

Secure backups и «мертвая рука» публикаций

- **Если вас отключат — правда всё равно выйдет**

- Хранить резервные копии в шифрованных облаках
- Настроить «dead man’s switch» (автопубликация)
- Распределить доступ между доверенными лицами

Legal core:

Право на свободу выражения (ст. 10 ЕКПЧ)

«Мёртвая рука» = материалы автоматически публикуются, если человек исчезает

Частые ошибки:

- **хранить единственную копию «у себя»**

Анти-фишинг и анти-слежка: практические фильтры

Письмо с поддельным логотипом может стоить свободы

- Проверять отправителя и домен
- Использовать двухфакторную аутентификацию
- Устанавливать анти-шпионские приложения

Фишинг и слежка — главный инструмент служб

Частые ошибки:

- **переходить по ссылкам из писем «банка/посольства»**

Legal core:

Кибербезопасность = обязанность государства (ООН резолюции)

Как читать лог-файлы и метки гео в медиафайлах

Каждое фото расскажет больше, чем вы думаете

- Проверять EXIF через специальные программы
- Чистить метаданные перед публикацией
- Сохранять оригиналы для суда

Legal core:

Приемлемость цифровых доказательств в судах (ЕСПЧ практика).

Фото и видео содержат EXIF-метки (место, время, устройство). Это может стать как доказательством, так и компроматом.

Частые ошибки:

- **выкладывать «сырые» фото без очистки данных**

Безопасные платежи и донаты: не спалить сеть

Ваш донат может выдать всю сеть

- Использовать анонимизированные шлюзы (PayPal alternatives, крипто-миксеры — где легально)
- Делить платежи на малые суммы
- Документировать каждую транзакцию для отчётности

Переводы и крипто-донаты часто раскрывают участников команды

Частые ошибки:

- **прямые переводы с личной карты**

Legal core:

AML/KYC стандарты + FATF рекомендации

Док-менеджмент для команды: роли и доступы

- Хранить кейсы в зашифрованных облаках (Proton Drive, Tresorit, Nextcloud)
- Разделить доступ: администратор / редактор / просмотр
- Вести лог действий (скачивание, изменения, время)
- Использовать пароль-менеджеры и 2FA
- Дублировать важные документы в офлайн-архиве (зашифрованный носитель)

Legal core:

GDPR (право на защиту данных), стандарты ISO/IEC 27001 по информационной безопасности

В любой правозащитной или юридической команде действует правило: информация делится по принципу «необходимого доступа». Если все видят всё, риск утечки максимален. Грамотный документооборот — это не только удобство, но и защита от компромата и атак

Частые ошибки:

- **Один общий пароль на всю команду**
- **Сохранение архива в «открытом» Google Drive**
- **Отсутствие резервного копирования**

ОСТАЛИСЬ ВОПРОСЫ?

наши контакты

ARGA OBSERVATORY

www.argaobservatory.org

Youtube

info@argaobservatory.org