



Observatoire ARGA

МЕЖДУНАРОДНЫЙ АНАЛИТИЧЕСКИЙ ДОКЛАД

D-24. Экспортный контроль

Технологии кибернаблюдения

Регламент (ЕС) 2021/821 и позиция ARGA

Автор:

Сергей Храбрых - президент ARGA, PhD

Организация: Observatoire ARGA

Адрес для корреспонденции: 21 rue de l'Aviation, 64600 Anglet, France

Контакты: info@argaobservatory.org, +33 7 58 49 62 27

Сайт: www.argaobservatory.org

28 сентября 2026 года

Содержание

Резюме	3
1. Предмет исследования и иерархия источников	3
2. Что считается средством кибернаблюдения	4
3. Три разных порога статьи 5	5
4. Оценка прав человека и конечного использования	6
5. Приложение I: техническая классификация	7
6. Удалённый доступ, облако и передача технологии	8
7. Участники сделки и применимая юрисдикция	9
8. Проверка конечного пользователя	10
9. Источники риска и качество доказательств	11
10. Обращение в компетентный орган	12
11. Разрешение, его пределы и независимые ограничения	13
12. Договорные условия и технические ограничения	14
13. Контроль после поставки и управление изменениями	15
14. Сообщение о злоупотреблении: порядок действий	16
15. Документирование и доказуемость решения	17
16. Что показывают официальные меры и судебная практика	18
17. Исследования безопасности и защита данных	19
18. Шесть практических ситуаций	20
19. Внутренняя программа и распределение ответственности	21
20. Протокол решения по конкретной поставке	22
21. Поэтапная поставка и проверка эффективности мер	24
22. Позиция ARGA и программа внедрения	25
Источники и справочный аппарат	26

Срез источников: 28 сентября 2026 года. Ключевые слова: экспортный контроль; кибернаблюдение; статья 5; права человека; конечный пользователь; должная проверка.

Резюме

Экспортный контроль технологий кибернаблюдения начинается с вопроса о том, какую возможность поставщик передаёт конкретному пользователю. Название продукта, регистрация покупателя и наличие гражданского договора по отдельности этого не объясняют. Один и тот же коммерческий пакет может включать обычную сетевую аналитику, контролируемый модуль, удалённую активацию дополнительной функции и услуги интегратора. Правовая оценка должна связывать эти элементы с техническими характеристиками, маршрутом передачи и предполагаемым использованием.

Регламент (ЕС) 2021/821 устанавливает два принципиально разных пути контроля. Для продукции из приложения I исходным основанием служит её классификация. Для не включённых в перечень средств кибернаблюдения статья 5 предусматривает специальный механизм, связанный с внутренними репрессиями и серьёзными нарушениями прав человека и международного гуманитарного права. Отсутствие позиции в приложении I поэтому не завершает проверку, но и потенциальная пригодность любого программного обеспечения для наблюдения сама по себе не создаёт универсального лицензионного требования. [1-3]

Доклад развивает позицию ARGА вокруг трёх требований: точная техническая квалификация, проверяемая оценка конечного использования и действенные меры после поставки. Предлагаемый подход не подменяет решение компетентного органа корпоративным заключением. Он определяет, какие факты компания должна собрать, как разрешать противоречия и какие действия допустимы до получения ответа. Рекомендация Комиссии 2024/2659 используется как официальный, но юридически необязательный ориентир для применения статьи 5. Авторские организационные предложения прямо отделены от требований Регламента. [2]

Практическая часть включает модель лицензионного досье, проверку посредников, управление обновлениями, работу с сообщениями о злоупотреблениях, шесть ситуационных разборов и последовательность внедрения контроля. Особое внимание уделено границам доказанности. Административное включение в ограничительный список, парламентская рекомендация и судебное решение имеют разное значение. Ни одно из них нельзя представлять как автоматическое доказательство нарушения статьи 5 в другой сделке.

1. Предмет исследования и иерархия источников

Правовой центр доклада - экспорт из Европейского союза продукции двойного назначения, способной обеспечивать скрытое наблюдение за физическими лицами. Рассматриваются также внутрисоюзные передачи, посреднические услуги и техническая помощь, когда соответствующая операция подпадает под самостоятельные положения Регламента. Эти режимы нельзя объединять только потому, что экономически они относятся к одному проекту. В каждом случае необходимы собственные территориальные, предметные и персональные основания. [1]

Основной источник - Регламент 2021/821 и применимые изменения его приложений. Для технической классификации существенна редакция перечня на дату операции: ежегодное обновление способно изменить ответ без изменения коммерческого наименования товара.

Делегированный регламент 2025/2003 обновил приложение I; регламент 2026/1405 исправляет отдельные языковые версии. Последний не следует представлять как самостоятельную реформу контроля кибернаблюдения. Доклад использует нормативные материалы, доступные на 28 сентября 2026 года. [1, 3, 4]

Следующий уровень - официальные рекомендации и разъяснения. Документы Комиссии помогают понять ожидания регулятора, но не создают новую уголовную ответственность и не отменяют национальные правила. Французские материалы SBDU используются для объяснения административного маршрута; они не превращаются в единый процессуальный кодекс для всех государств ЕС. Американские меры рассматриваются сравнительно, с указанием их собственного правового охвата. [2, 5-8]

Метод исследования сочетает анализ норм и построение проверяемой процедуры принятия решений. Предлагаемые формы досье, сроки внутренней реакции и критерии аудита являются рекомендациями ARGА. Шесть ситуаций в разделе 18 условны: они показывают изменение решения при изменении фактов и не описывают реальные компании. Такая форма позволяет обсуждать практику без вымышленных судебных прецедентов, статистики отказов или утверждений о неизвестных обстоятельствах закрытых лицензий.

Отдельный вопрос - время действия вывода. Историческое сообщение подтверждает принятие меры в определённую дату, но без актуальной проверки не устанавливает сегодняшние ограничения каждого названного лица. Классификационное заключение также относится к описанному продукту и правовой редакции. При реальной операции необходимо проверить, сохранились ли факты, на которых основано решение.

2. Что считается средством кибернаблюдения

Статья 2(20) связывает понятие средств кибернаблюдения с продукцией двойного назначения, специально разработанной для скрытого наблюдения за физическими лицами посредством мониторинга, извлечения, сбора или анализа данных информационных и телекоммуникационных систем. Перечисленные операции альтернативны: не обязательно одновременно перехватывать, хранить и анализировать данные. Вместе с тем отдельная возможность обрабатывать информацию не отменяет остальных элементов определения. [1, 2, раздел 1.2]

Рекомендация 2024/2659 предлагает оценивать объективные технические свойства и основную цель разработки. Продукт может иметь несколько применений и всё же быть специально разработанным для скрытого наблюдения. Обратная ситуация также возможна: промышленный мониторинг или обычная защита сети не становятся средствами кибернаблюдения исключительно из-за гипотетической возможности злоупотребления. Маркетинговое слово «безопасность» не решает ни одну из этих задач. Инженер должен объяснить, какие функции существуют в поставляемой версии и для чего они были созданы. [2]

Скрытый характер наблюдения не ограничивается невидимой установкой программы на телефон. Руководство Комиссии допускает, что данные из публичного пространства используются способом, которого человек объективно не ожидает. Поэтому видимая камера и незаметная последующая идентификация образуют разные аналитические вопросы.

Обычная камера не должна автоматически квалифицироваться как контролируемая система; интегрированное решение с дополнительной аналитикой требует самостоятельного рассмотрения. [2, разделы 1.2 и 2.2]

Практически полезен функциональный паспорт. Он содержит описание обрабатываемых данных, способ определения человека, пределы доступа, состав модулей, возможность удалённого включения функций и фактическую роль оператора. К паспорту прилагаются спецификация и результаты демонстрации в контролируемой среде. Недостаточно фразы «персональные данные не собираются», если система связывает устойчивый идентификатор устройства с перемещениями конкретного человека. Равным образом нельзя объявлять идентификацией человека каждый технический журнал без анализа его содержания.

Проверка должна охватывать готовую конфигурацию. Если поставщик передаёт несколько компонентов, заранее предназначенных для совместной работы, анализ каждого изолированно может скрыть значимую функцию системы. Однако интеграция не означает, что любой универсальный компонент автоматически приобретает классификацию конечного комплекса. В досье фиксируются роль компонента, известная конфигурация и правовое основание вывода. Это позволяет обосновать решение и о контролируемости, и об отсутствии соответствующего основания.

Полезно заранее назвать обстоятельства, которые изменят вывод. Добавление идентификации, включение скрытой функции или существенное изменение назначения разработки должны запускать пересмотр, если они влияют на квалификацию. Именно эти границы делают технический паспорт полезным. Узкое заключение о конкретной версии надёжнее общего заверения обо всей линейке.

3. Три разных порога статьи 5

Первый путь предусмотрен статьёй 5(1): экспортёр получает от компетентного органа информацию, что не включённые в приложение I средства кибернаблюдения предназначены или могут предназначаться полностью либо частично для соответствующего опасного использования. При таком уведомлении требуется разрешение. Корпоративная оценка низкого риска не отменяет индивидуальное действие органа. Необходимо установить, какую продукцию, пользователя и операцию охватывает полученная информация. [1]

Второй путь - статья 5(2). Когда экспортёру по результатам должной проверки известно о предназначении продукции для названного использования, он уведомляет компетентный орган. Орган решает, ставить ли соответствующий экспорт под разрешительный контроль. Следовательно, уведомление экспортёра и уже возникшая обязанность получить разрешение по пункту 1 - не одно и то же юридическое событие. Внутренняя политика должна отражать последовательность, а не заменять её неопределённой отметкой «санкционный риск». [1, 2]

Руководство Комиссии связывает осведомлённость с положительным знанием о предполагаемом злоупотреблении. Одна теоретическая возможность недостаточна. Но это не оправдание пассивности: экспортёр должен предпринять действия, позволяющие получить достаточные сведения о сделке. В практическом досье поэтому различаются известный факт, обоснованный вывод и неразрешённый вопрос. Уверенность сотрудника без источника не

заменяет знания; сознательный отказ читать доступные существенные сведения не является качественной проверкой. [2, раздел 1.2.6]

Третий путь предусмотрен статьёй 5(3): государство-член может установить национальное требование разрешения при наличии у экспортёра оснований подозревать соответствующее использование. Это возможность национального законодателя, а не автоматически одинаковый для всего ЕС стандарт. Проверка должна установить, воспользовалось ли им применимое государство и в какой форме. Нельзя механически перенести национальный порог подозрения в описание пункта 2 или считать отсутствие доказанного знания разрешением не исследовать явно противоречивую сделку. [1]

Для управления неопределённостью ARGА рекомендует внутреннюю приостановку соответствующей передачи до разрешения существенного вопроса. Такая мера может быть шире прямо установленного законом запрета. В решении следует честно указать её основание: обязательное лицензионное требование, необходимость уведомления органа либо корпоративная оценка неприемлемого риска. Это важно и для руководства, и для контрагента, который должен понимать, какое условие действительно способно изменить результат.

Приостановка должна иметь определённый предмет. Запрет активировать спорный модуль не обязательно требует прекратить все независимые услуги клиенту. Но сохранение эквивалентного канала передачи может сделать ограничение фиктивным. В решении фиксируются удерживаемая возможность, лицо, уполномоченное снять ограничение, и необходимые для пересмотра факты.

4. Оценка прав человека и конечного использования

Статья 5 посвящена определённым видам опасного использования, а не общей моральной оценке страны. Внутренние репрессии могут включать произвольные задержания, пытки и другие тяжёлые посягательства на основные права. При анализе необходимо показать причинную связь между функцией поставляемой системы, полномочиями пользователя и конкретным риском. Ссылка на неблагоприятный политический контекст усиливает внимание, но не заменяет такой связи. [1, 2, раздел 1.3]

Например, программа может позволять устанавливать контакты журналиста с источниками. Значимы не только точность её работы, но и правовые основания выбора объекта, круг лиц с доступом к результатам, сроки хранения и возможность независимого обжалования. Заявление заказчика о борьбе с терроризмом требует проверки по существу: какая процедура ограничивает использование продукта и кто контролирует соблюдение ограничений. Общая государственная компетенция не равна разрешению на любое вмешательство.

Международное гуманитарное право требует отдельного контекста вооружённого конфликта. Не каждое нарушение неприкосновенности частной жизни автоматически является нарушением этого права. В то же время сведения о местонахождении гражданских лиц могут приобретать непосредственное значение для угроз их жизни. Аналитик должен установить применимую правовую рамку, характеристики пользователя и предполагаемое применение данных, не подменяя квалификацию эмоциональным описанием технологии. [2]

Оценка серьёзности должна учитывать масштаб, тяжесть и возможность исправления последствий. Небольшое число объектов наблюдения не делает риск несущественным, если речь идёт об опасности попыток или раскрытии защищаемых источников. Коммерческая стоимость сделки также не является мерой вреда. Предложение ARGА состоит в том, чтобы отдельно фиксировать риск для людей и риск для компании. Иначе потенциально тяжёлый вред растворяется в средней оценке, где его компенсируют доходность и привлекательность рынка.

Должная проверка в области прав человека по Руководящим принципам ООН шире одного лицензионного вопроса. Она включает выявление воздействия, принятие мер и отслеживание их результатов. Эти принципы сами по себе не заменяют нормативных условий статьи 5 и не являются отдельной экспортной лицензией. Их значение для рассматриваемой процедуры - помочь оценивать последствия поставки за пределами момента пересечения границы. [9]

Значение имеют действующие гарантии, а не только их наличие в законе или корпоративной политике. Если пользователь ссылается на независимое санкционирование, следует получить соразмерное подтверждение того, как оно применяется к проекту. Цель - не массовый сбор секретных оперативных документов, а проверка реальности ограничений, на которых строится оценка риска.

5. Приложение I: техническая классификация

Первая предметная проверка касается действующего приложения I. В официальном руководстве по кибернаблюдению приведены, среди прочего, позиции для отдельных систем перехвата телекоммуникаций, интернет-наблюдения, оборудования и программного обеспечения, связанного с intrusion software, а также некоторых средств криптоанализа и цифровой криминалистики. Это ориентиры для поиска, а не сокращённый альтернативный перечень. Полные технические условия, определения и примечания необходимо читать вместе. [1-3]

Номер категории нельзя присваивать по названию отрасли. Продукт, называемый forensic tool, может отличаться способом извлечения данных, поддерживаемыми устройствами и обходом защитных механизмов. Аналогично термин intrusion software в приложении работает внутри конкретных контрольных позиций; он не означает, что всякая программа тестирования безопасности запрещена. Заключение должно называть позицию, сопоставлять каждый существенный признак и объяснять применимость примечаний.

Полезен двусторонний формат классификационной записки. Инженер отвечает за достоверность технических характеристик, специалист по экспортному контролю - за их сопоставление с нормой. Владелец продукта подтверждает состав продаваемой версии. Если будущая функция ещё не включена, но передаваемый ключ позволяет её активировать, это обстоятельство отражается отдельно. Нельзя ссылаться на ограниченную демонстрационную версию, когда договор фактически предусматривает передачу более широких возможностей.

Изменение перечня, версии продукта или существенного технического параметра запускает повторную проверку. Для уже разрешённой операции оцениваются условия разрешения и применимые переходные положения, если они существуют. Доклад не предполагает, что любое обновление автоматически требует новой лицензии: такой вывод зависит от

содержания передачи и действующих условий. Однако отсутствие физической посылки не позволяет исключить экспорт программного обеспечения или технологии.

Результат классификации должен быть воспроизводим. В архиве остаются редакция приложения, описание конфигурации, дата анализа, ответственный специалист и существенные допущения. Внешнее заключение консультанта полезно, если оно относится к фактической версии и раскрывает логику. Формула «аналогичный продукт ранее не контролировался» не отвечает на вопрос, совпадают ли характеристики, маршрут и правовая редакция.

Для продукта из сторонних модулей классификация изготовителя является существенным, но не всегда окончательным доказательством в отношении объединённого предложения. Интеграция может изменить предмет передачи, а неверное описание компонента - исказить весь анализ. Компания собирает сведения, достаточные для собственного решения, и запрашивает компетентное разъяснение при существенной технической неопределённости.

6. Удалённый доступ, облако и передача технологии

Определение экспорта в Регламенте охватывает не только физическое перемещение, но и определённые электронные передачи программного обеспечения или технологии за пределы таможенной территории Союза, включая предоставление доступа в предусмотренных нормой случаях. Поэтому электронная почта, репозиторий, сервер обновлений и удалённая демонстрация требуют внимания наравне с отгрузкой оборудования. При этом нельзя утверждать, что любой доступ иностранного клиента к любому облачному сервису автоматически является контролируемым экспортом. [1, статья 2]

Анализ начинается с карты передачи. Что именно получает адресат: исполняемый модуль, исходный код, техническую документацию, возможность управлять системой или только результат обработки? Где находятся передаваемый объект и получатель? Кто определяет доступ? Какую юридическую и техническую роль играет облачный оператор? Ответы помогают отделить передачу контролируемого объекта от услуги, для которой могут действовать другие нормы. География сервера сама по себе не разрешает весь вопрос.

Для репозитория существенны фактические права. Формально доступ предоставлен европейскому интегратору, но его команда может находиться в третьей стране и иметь разрешение выгружать материалы. Обратная ситуация: зарубежный посетитель получает только публичную инструкцию без контролируемой технологии. Обе операции требуют анализа содержания, а не реакции на иностранное гражданство. Европейские правила нельзя механически описывать через американскую концепцию *deemed export*: юрисдикционные основания различаются.

Внутренний контроль должен срабатывать до предоставления доступа. ARGA предлагает связывать разрешённую конфигурацию с учётной записью, страной использования, юридическим лицом и сроком действия согласования. Изменение одного из существенных параметров направляется на повторную оценку. Это не требование создавать повсеместное наблюдение за сотрудниками. Достаточно минимальных журналов выдачи прав, версий и получателей, позволяющих подтвердить, какая возможность действительно была передана.

Обновления безопасности требуют особенно аккуратного решения. Они могут снижать риск для пользователей, но одновременно содержать новые контролируемые функции. Следует разделять исправление уязвимости, расширение возможностей и техническую помощь. Если возникает правовое препятствие, компания обсуждает с компетентным органом допустимый способ устранения опасности. Самовольная отправка под предлогом защиты и безусловное прекращение всех исправлений одинаково плохо заменяют предметный анализ.

Удалённая демонстрация также требует предметной оценки. Ограниченная презентация и полноценное эксплуатационное испытание предоставляют разные возможности. Название сессии не решает, происходит ли передача контролируемого объекта. В досье сохраняются границы доступа, чтобы правовой вывод можно было сопоставить с фактическими действиями участников.

7. Участники сделки и применимая юрисдикция

Экспортёр определяется по юридическим критериям Регламента, включая полномочие принимать решение о передаче в соответствующих случаях. Выбор того, кто выставляет счёт, не всегда отвечает на этот вопрос. В сложной группе договор заключает одна компания, продукт контролирует другая, а доступ выдаёт третья. Необходимо зафиксировать реальные полномочия и распределение действий. Внутригрупповое соглашение может распределять работу, но не переписывает обязательные определения. [1, статья 2]

Проверка посредника охватывает его коммерческую роль, собственников, фактических операторов и способность выполнять заявленный проект. Посредник, не обладающий техническим персоналом, может законно заниматься перепродажей. Однако требование скрыть конечного пользователя, несоразмерное вознаграждение или необъяснимый маршрут требуют выяснения. Ни один признак по отдельности не является автоматическим доказательством обхода; их сочетание может сделать исходное объяснение сделки неправдоподобным.

Статьи о посредничестве, технической помощи и транзите имеют самостоятельные условия. Нельзя автоматически переносить специальный режим статьи 5 на любую консультацию по тому же продукту. В то же время действия могут подпадать под другие положения Регламента, национальный контроль или санкции. Досье должно содержать отдельную таблицу операций: экспорт модуля, предоставление доступа, обучение, последующая поддержка и передача внутри ЕС. Для каждой указывается основание проверки. [1, статьи 6-11]

Внутри Союза не действует универсальная свобода передачи любой контролируемой продукции. Приложение IV и статья 11 предусматривают специальные случаи, а некоторые обстоятельства дальнейшего экспорта также требуют внимания. Но сама маркировка «кибернаблюдение» не означает, что всякая внутрисоюзная передача лицензируется. Оценка строится по конкретному правилу. Такой подход препятствует как необоснованным запретам, так и использованию европейского посредника для игнорирования известного конечного маршрута.

Американская связь анализируется отдельно: происхождение компонентов, статус продукции по EAR, участники и иные применимые основания. Проверка OFAC не подменяет

проверку BIS, а европейская лицензия не снимает самостоятельное американское ограничение. Описывать все эти режимы как один «международный запрет» юридически неточно. Для руководства полезнее несколько ясных выводов с указанием применимости, чем один непрозрачный цветовой рейтинг.

При обращении к нескольким органам фактические описания должны быть согласованы. Разные версии конечного пользователя или функций продукта подрывают достоверность процедуры. Согласованность не означает одинаковый результат в разных режимах: различие должно объясняться применимым правом, а не выборочным представлением обстоятельств.

8. Проверка конечного пользователя

Наиболее важный документ сделки - не всегда контракт с покупателем. Конечным пользователем может быть государственное подразделение или оператор, который в нём прямо не назван. ARGA предлагает устанавливать четыре роли: кто платит, кто получает продукт, кто управляет системой и кто принимает решения о наблюдении. Если роли разделены, объяснение должно подтверждаться документами и совпадать с технической схемой развёртывания.

Заявление о конечном использовании должно описывать функцию, место эксплуатации, операторов и ограничения дальнейшей передачи. Общая фраза «для обеспечения национальной безопасности» слишком широка для проверки. Более содержательный документ указывает компетенцию подразделения, категории разрешённых задач, порядок санкционирования доступа и запрет передачи иным операторам без согласованной процедуры. Само заявление остаётся доказательством позиции заказчика, а не независимым подтверждением её истинности.

Проверяется согласованность источников. Если закупка оформлена для телекоммуникационной компании, а обучение запрашивает подразделение другого ведомства, необходимо установить его роль. Если заказчик требует число лицензий, многократно превышающее потребности заявленного подразделения, выясняется архитектура проекта. Техническая особенность может иметь невинное объяснение, но оно должно быть конкретным. Ответ посредника «так принято на местном рынке» не закрывает вопрос о фактическом операторе.

Проверка собственников и контролирующих лиц особенно важна при санкциях, однако перечень бенефициаров не заменяет исследование использования продукта. Полностью прозрачная компания может обслуживать опасного конечного пользователя; сложная группа может иметь законную структуру. Следует избегать презумпции виновности по организационной форме. Вывод основывается на совокупности фактов, а отказ предоставить существенные сведения учитывается как ограничение возможности принять положительное решение.

Государственный заказчик может ссылаться на секретность. Это не обязывает поставщика требовать раскрытия оперативных объектов, но и не позволяет пропустить проверку. Возможны подтверждение полномочий компетентным органом, ограниченный доступ проверяющего к документам и описание системы надзора без раскрытия операций. Если

даже минимальные сведения о пользователе и назначении недоступны, компания должна признать предел проверки и решить вопрос с регулятором либо отказаться от сделки.

Правовые полномочия заказчика следует отличать от технического доступа. Подразделение с установленной компетенцией может допускать к системе подрядчиков или другие ведомства. Технический администратор, напротив, может обслуживать инфраструктуру, не выбирая объекты наблюдения. В обоих случаях необходимо объяснить распределение функций: одного наименования покупателя недостаточно.

9. Источники риска и качество доказательств

Досье не должно превращаться в подборку отрицательных публикаций. Для каждого существенного сообщения фиксируются автор, дата, первоисточник, описанный период и связь с конкретной организацией. Несколько материалов, пересказывающих одно расследование, не являются несколькими независимыми подтверждениями. Опровержение также оценивается по содержанию: предъявленные документы имеют больший вес, чем общее отрицание без ответа на установленные обстоятельства.

Техническое исследование может надёжно выявить следы определённого инструмента, но не всегда устанавливает заказчика, оператора или правомерность конкретного применения. В отчёте необходимо различать атрибуцию продукта, инфраструктуры и ответственного лица. Ошибка на этом этапе способна повредить и объекту наблюдения, и неправомерно обвинённой компании. Для экспортного решения иногда достаточно серьёзной неопределённости, требующей приостановки, хотя доказательств для публичного обвинения ещё нет.

ARGA предлагает вести журнал нерешённых вопросов. Каждая запись содержит факт, его потенциальное значение, источник, требуемое уточнение и ответственного. Например, несовпадение адреса установки не обозначается просто как «высокий риск»: указывается, почему оно может свидетельствовать о другом операторе, какое подтверждение запрошено и какое действие временно ограничено. Такой формат позволяет проверять качество решения, а не количество собранных страниц.

Риск нельзя безусловно усреднять. Подтверждённое намерение использовать средство для преследования конкретной группы не нейтрализуется хорошей финансовой отчётностью покупателя. В то же время слабый неподтверждённый сигнал не должен навсегда блокировать законную поставку. Для каждого вывода предусматриваются условия пересмотра: независимое подтверждение пользователя, изменение конфигурации, решение компетентного органа либо устранение неверного совпадения при проверке списка.

Сбор сведений должен учитывать безопасность источников. Нельзя направлять потенциальному оператору наблюдения имена заявителей или подробности, позволяющие установить пострадавшего, только ради получения комментария. Запрос контрагенту формулируется так, чтобы проверить существенный факт с минимальным раскрытием. Если безопасная проверка невозможна, это ограничение учитывается в решении; оно не компенсируется созданием нового риска для человека.

При итоговой проверке полезно спросить, не сильнее ли вывод, чем доказательства. Вероятная причастность продукта, установление оператора и незаконность применения - разные утверждения. Профилактическое действие допустимо обосновывать неопределённостью, не выдавая её за доказанный факт. Решение должно точно показывать, какое утверждение поддержано материалами.

10. Обращение в компетентный орган

Во Франции SBDU выполняет функции компетентного органа по классификации и выдаче экспортных лицензий на продукцию двойного назначения. Официальные материалы предусматривают использование технических описаний, договорных документов и сведений о конечном назначении в зависимости от характера обращения. Передача неполного рекламного буклета затрудняет ответ: органу необходимо понимать фактическую операцию, а не только сектор бизнеса заявителя. [5-7]

Досье ARGА начинается с краткого описания требуемого решения. Компания указывает, обращается ли за классификацией, уведомляет по статье 5(2), подаёт лицензионное заявление или сообщает об изменении уже согласованной сделки. Затем следуют технический паспорт, карта участников, маршрут передачи, оценка использования и существенные противоречия. Правовая позиция сопровождается документами, которые позволяют проверить её исходные факты.

Особое значение имеет полнота негативной информации. Если внутреннее заключение опиралось на спорный факт, его нельзя удалить из пакета только потому, что он осложняет получение разрешения. Вместо этого указываются источник, оценка надёжности и ответ заказчика. Неизвестное обозначается как неизвестное. Компетентный орган может располагать дополнительными сведениями; сокрытие существенного вопроса лишает процедуру её профилактического смысла.

Блок досье	Что подтверждается	Практический результат
Продукт и версия	Функции, модули, технические параметры	Воспроизводимая классификация
Участники и маршрут	Получатель, оператор, посредники, доступ	Определение применимых режимов
Конечное использование	Задача, правовые основания, ограничения	Оценка риска злоупотребления
Проверка и противоречия	Источники, ответы, нерешённые вопросы	Осознанное решение органа
Условия исполнения	Этапы, обновления, контроль передачи	Возможность соблюдать разрешение

Переписка с органом сохраняется вместе с версией досье. Если ответ основан на конкретной конфигурации, изменение пользователя или функций требует проверки его применимости.

Не следует представлять предварительную консультацию как безусловную лицензию. Также нельзя устанавливать собственный срок, по истечении которого молчание органа считается одобрением, если применимое право прямо не предусматривает такой эффект.

Техническую сложность следует объяснять, а не скрывать. Краткое описание функции, оператора и гарантий дополняется подробной спецификацией. Успокаивающие формулировки вместо фактов затрудняют оценку. Обратная крайность - неструктурированная масса документов - также мешает увидеть конкретный вопрос, по которому требуется решение органа.

11. Разрешение, его пределы и независимые ограничения

Статья 15 требует учитывать релевантные обстоятельства, включая международные обязательства, санкции, соображения внешней политики и безопасности, конечное использование и риск отклонения от него. Лицензия поэтому не является чисто техническим свидетельством соответствия продукта. Вид разрешения и его условия определяют, какие операции, получатели, объёмы и сроки охвачены. Право пользоваться общей авторизацией также зависит от её собственных условий и исключений. [1]

Лицензионная карточка должна быть доступна тем, кто фактически исполняет сделку. В ней отражаются разрешённая версия, пользователь, страна, срок, ограничения поддержки и необходимые отчётные действия. Бухгалтеру недостаточно увидеть номер разрешения; инженер должен знать, какие функции можно активировать. Если условия непонятны технической команде, вероятность нарушения сохраняется даже при аккуратно оформленном юридическом архиве.

Разрешение по правилам двойного назначения не подтверждает законность обработки персональных данных, правомерность наблюдения в государстве назначения или отсутствие санкционного запрета. Во Франции регулирование криптографии и компетенция ANSSI также требуют отдельной оценки по применимым правилам; экспортная лицензия SBDU не должна изображаться универсальным разрешением на все аспекты продукта. [8] Разделение проверок позволяет ясно увидеть, какой именно вопрос остаётся нерешённым.

После получения разрешения существенное изменение фактов нельзя игнорировать. Новая информация о пользователе, изменение маршрута или добавление функций могут потребовать обращения к органу, пересмотра внутреннего решения либо иного действия согласно условиям лицензии. Нельзя утверждать, что сама выдача разрешения гарантирует допустимость любых будущих поставок тому же клиенту. Каждая операция должна попадать в фактические и правовые границы разрешённого.

Внутренний отказ может сохраняться и при отсутствии прямого запрета. Компания вправе устанавливать более строгую политику, соблюдая применимые договорные и иные обязательства. В таком случае честная формулировка решения особенно важна: отказ объясняется корпоративным стандартом или неустранимым риском, а не вымышленным требованием государства. Это повышает качество диалога с заказчиком и не искажает содержание права.

Для каждого условия отчётности или подтверждения использования назначается исполнитель. Задача не должна исчезать между юридической, инженерной и операционной командами. В карточке отражаются момент проверки и доказательство выполнения. Условие, существующее только в архивном тексте лицензии, легко теряется при обновлении или смене персонала.

12. Договорные условия и технические ограничения

Договор нужен для закрепления проверенной модели использования. Он должен определять согласованного пользователя, конфигурацию, территорию эксплуатации и процедуру изменения этих параметров. Запрет незаконного наблюдения полезен, но слишком общий, если не установлено, кто подтверждает соблюдение и какие сведения доступны поставщику. Практический смысл имеет сочетание понятного обязательства с исполнимым механизмом проверки.

ARGA рекомендует согласовывать запрет неразрешённой дальнейшей передачи, обязанность сообщать о смене оператора и право приостановить конкретные поставки при существенном несоответствии. При этом полномочия поставщика не должны быть безграничными. Порядок запроса документов, сроки ответа, защита секретной информации и возможность независимой проверки делают условие более реалистичным. Одностороннее право требовать любые данные в любое время часто оказывается непригодным для исполнения.

Технические меры оцениваются по способности снижать установленный риск. Разделение прав операторов, ограничение активируемых модулей, журнал изменения конфигурации и отдельное согласование расширения доступа могут быть полезнее абстрактного обещания «этичного использования». Однако географическое ограничение не гарантирует, что информация не будет использована против человека в другой стране. Проверка должна объяснять, какой риск мера уменьшает и какой остаётся.

Механизм удалённого отключения нельзя считать универсальным решением. Его наличие может создавать дополнительную уязвимость, конфликтовать с договором или причинить вред законным пользователям. Если он предусмотрен, необходимы заранее определённые основания, полномочия, безопасный порядок исполнения и оценка последствий. Контроль не должен зависеть от скрытой функции, о которой ответственные стороны не знают. Техническая возможность остановки также не заменяет правового основания для её использования.

Договор не устраняет знание о предполагаемом злоупотреблении. Если существенные факты указывают на опасное назначение, подписанная стандартная декларация не возвращает сделку автоматически в низкую категорию риска. С другой стороны, реально изменённая конфигурация может повлиять на оценку: например, исключение спорного модуля, подтверждённое независимой проверкой, имеет иной вес, чем обещание его не включать. Такое изменение оценивается заново и документируется.

Договорные средства оцениваются с учётом реального влияния поставщика. После автономной установки обещание дальнейшего сотрудничества может оказаться трудноисполнимым. Этот предел учитывается до поставки. Никакая договорная формула не создаёт технического контроля или законного доступа, которых у компании фактически нет.

13. Контроль после поставки и управление изменениями

Риск развивается вместе с продуктом и заказчиком. Система, приобретённая для одной задачи, может получить новые модули, попасть к иному оператору или использоваться в изменившейся политической обстановке. Поэтому проверка только при первой продаже недостаточна как организационная модель. Вместе с тем статья 5 не должна описываться как безусловное требование непрерывно наблюдать за каждым действием клиента. Конкретные юридические обязанности определяются нормой, лицензией и применимыми национальными правилами.

Предлагаемая ARGА модель строится вокруг событий. Повторный анализ запускают смена конечного пользователя, существенное расширение функции, новый маршрут доступа, достоверное сообщение о злоупотреблении или изменение ограничительного режима. Коммерческая команда сообщает о событиях, но не принимает единолично решение о продолжении. При обычном продлении неизменённой услуги объём проверки может быть меньше, чем при новом развёртывании, если это обосновано актуальностью сведений.

Инженерная поддержка часто первой замечает расхождение с заявленным использованием. Запросы на изменение журналирования, расширение числа операторов или перенос активации в другую страну могут быть важны для оценки. Сотрудника не следует превращать в следователя: его задача - зафиксировать фактическое изменение и передать его ответственному специалисту. Для этого нужна понятная форма сообщения и защищённый от коммерческого давления порядок рассмотрения.

Если продукт работает автономно и поставщик больше не имеет технического доступа, нельзя обещать полный контроль конечного использования. В досье прямо указываются пределы наблюдаемости. Возможные меры - периодическое подтверждение пользователя, независимый аудит или обусловленное предоставление новых функций. Их выбор зависит от риска и реальной исполнимости. Недоступность идеального контроля не оправдывает ложные заверения о его наличии.

Контроль поддержки должен учитывать возможный вред прекращения. Отказ от расширения функциональности и отказ от исправления уязвимости имеют разные последствия. Решение описывает, какие действия приостанавливаются, что необходимо для сохранения безопасности и требуется ли согласование с органом. Такая точность помогает избежать ситуации, когда борьба со злоупотреблением сама приводит к утечке данных или разрушению доказательств.

После устранения вопроса необходим формальный путь к возобновлению работы. Ответственный фиксирует доказательства, оставшиеся условия и доводит решение до исполнителей. Иначе устаревшее ограничение сохраняется бессрочно либо снимается неофициально. Оба исхода ослабляют доверие к системе.

14. Сообщение о злоупотреблении: порядок действий

Первое действие - обеспечить безопасное получение информации. Канал обращения должен позволять передать существенные сведения без обязательного раскрытия личности публично или потенциально заинтересованному клиенту. Получателю объясняют пределы конфиденциальности и не обещают абсолютную защиту, которую организация не способна гарантировать. Доступ к материалам ограничивается теми, кому он необходим для оценки и принятия решения.

Затем фиксируются время поступления, содержание сообщения и имеющиеся технические материалы. Оригиналы сохраняются отдельно от рабочих копий; документируются преобразования и лица, получавшие доступ. Проверяющий устанавливает, относится ли сообщение к продукту компании, какой версии и периоду. Не следует требовать от заявителя невозможного доказательства всей цепочки ответственности до начала первичного анализа. Предварительная техническая правдоподобность и риск для человека могут оправдывать немедленную внутреннюю эскалацию.

В первые рабочие действия входит проверка предстоящих передач. Если завтра запланировано расширение доступа тому же оператору, решение нельзя откладывать до завершения многомесячного расследования. Временная остановка соответствующего расширения может быть разумной корпоративной мерой. Юридическая команда одновременно устанавливает обязанности перед компетентными органами, условия лицензии и применимость правил о данных. Доклад не устанавливает универсального срока уведомления для всех возможных происшествий.

Связь с контрагентом организуется после оценки риска для заявителя и сохранности доказательств. Запрашивается объяснение конкретного несоответствия, а не передаётся весь полученный материал. Если ответ не подтверждён, это отражается в решении. Если он опровергает исходное предположение, ограничение может быть пересмотрено. Процедура должна допускать оба результата: её задача - достоверное решение, а не обязательное подтверждение первоначального подозрения.

Завершение проверки включает оценку исправительных мер и доступных способов содействия пострадавшим. В зависимости от обстоятельств это может быть сохранение доказательств, сотрудничество с законным расследованием, изменение продукта или помощь в безопасном устранении последствий. Не каждое предприятие обладает полномочиями определить компенсацию или раскрыть секретные сведения. Руководящие принципы ООН дают ориентир для ответственного поведения, но конкретные юридические обязанности и средства защиты устанавливаются применимым правом. [9]

В итоговой записи различаются установленные факты, нерешённые вопросы, принятые меры и основания будущего пересмотра. Невозможность установить оператора не означает автоматически необоснованность жалобы. Но нерешённое предположение также нельзя повторять как подтверждённый вывод. Организация объясняет, какие риски она смогла уменьшить в пределах своих полномочий.

15. Документирование и доказуемость решения

Статья 27 предусматривает ведение подробных записей или регистров экспортных операций и соответствующих документов. Для указанных в ней записей об экспорте, посреднических услугах и технической помощи установлен срок хранения не менее пяти лет с конца календарного года, когда состоялась операция. Внутрисююзные передачи имеют собственные требования; нельзя распространять одну формулу срока на весь архив без проверки. Национальные и иные применимые обязанности могут требовать дополнительного хранения. [1, статья 27]

Юридически полезное досье показывает не только итог, но и основания на дату решения. Оно содержит версию продукта, редакцию классификации, документы пользователя, существенные источники, ответы на вопросы, условия разрешения и фактические передачи. Позднее найденные сведения добавляются с датой, а не подменяют старую запись. Иначе невозможно отличить разумное решение при ограниченной информации от ретроспективно созданного оправдания.

Объём архива должен быть соразмерен цели. Экспортный контроль не требует по умолчанию сохранять содержание всех сообщений людей, наблюдаемых клиентом. Такое накопление само создаёт риск. При применимости GDPR необходимо определить основание обработки, минимизировать данные, ограничить доступ и установить обоснованные сроки. Факт потенциального судебного спора также не позволяет бессрочно хранить любые сведения без связи с конкретной необходимостью. [15]

Цифровой след важен на уровне действий: кто одобрил доступ, когда была активирована версия, какой получатель получил документацию. Контрольные суммы и журналы помогают подтвердить неизменность, но не доказывают истинность исходных сведений или законность их получения. Техническая целостность, достоверность содержания и юридическая допустимость - разные вопросы. Внутренний аудит должен проверять все три, если они существенны для рассматриваемой операции.

Сохранение материалов при инциденте организуется адресно. Ответственный определяет относящиеся к нему документы, предотвращает обычное удаление и фиксирует круг доступа. При этом исполнение законного запроса государственного органа и добровольная передача иностранному контрагенту имеют разные основания. Конфиденциальность юридической консультации также зависит от применимого режима; маркировка письма словом «привилегированное» сама по себе защиты не создаёт.

Досье должно быть понятно человеку, не участвовавшему в сделке. Цепочка подписей без причин решений слабо подтверждает реальную проверку. Краткое объяснение с сохранёнными первоисточниками позволяет установить и объём анализа, и его пределы. Цель - достоверно восстановить процесс, а не накопить максимальное число документов.

16. Что показывают официальные меры и судебная практика

В ноябре 2021 года BIS объявило о включении NSO Group и Candiru в Entity List, сославшись на сведения о поставке шпионских средств, использовавшихся иностранными правительствами против журналистов, активистов и других лиц. Мера касалась операций с продукцией, подпадающей под EAR, в соответствии с установленными лицензионными условиями. Это административная экспортная мера США, а не решение суда о нарушении европейской статьи 5. Для анализа сделки необходимо отдельно проверять актуальную запись и юрисдикционную связь. [10]

5 марта 2024 года OFAC объявило о санкциях против двух физических лиц и пяти организаций, связанных с консорциумом Intellexa. Казначейство США объяснило решение рисками и применением коммерческого шпионского ПО, включая угрозы американским лицам. Этот исторический акт показывает самостоятельность финансовых ограничений: экспортная классификация продукта и санкционный статус участника отвечают на разные вопросы. Описанная мера не означает, что все участники отрасли автоматически подпадают под одинаковые запреты; текущий статус проверяется на дату операции. [11]

Рекомендации Европейского парламента по итогам расследования PEGA в июне 2023 года поставили вопросы независимых расследований, гарантий, средств защиты и исполнения экспортных правил. Парламентский документ важен как институциональная оценка проблемы и направление публичной политики. Он не заменяет индивидуальное решение лицензирующего органа и не устанавливает уголовную виновность каждого упомянутого участника. Использование такого материала требует ясного указания его юридической природы. [12]

В деле *Big Brother Watch and Others v. the United Kingdom* Большая палата ЕСПЧ 25 мая 2021 года исследовала гарантии в режимах перехвата и связанные вопросы статей 8 и 10 Конвенции. Суд выявил недостатки, в том числе в независимом санкционировании и контроле использования идентификаторов, связанных с людьми, а также в защите журналистских материалов. Решение не является делом об экспортной лицензии; его практическая ценность здесь состоит в критериях оценки системы гарантий на протяжении обработки информации. [13]

Из этих материалов ARGА выводит организационный принцип: проверять не только объявленную цель приобретения, но и ограничения реальной эксплуатации. Это авторский вывод, а не цитата из единого международного стандарта. Административный акт может служить основанием обязательного ограничения в своей юрисдикции; судебное решение раскрывает правовой стандарт в рассмотренном контексте; парламентская рекомендация указывает на системную проблему. Смешение этих функций делает доклад громче, но юридически слабее.

История ограничительных мер не заменяет анализ конкретной операции. Значимы применимые меры и подтверждённые обстоятельства, относящиеся к участникам и передаваемой возможности. Исторический факт может иметь большой вес и одновременно требовать актуальной проверки. Качественное досье сохраняет и его значение, и границы выводов.

17. Исследования безопасности и защита данных

Контроль должен сохранять различие между средствами злоупотребления и законной исследовательской деятельностью. Приложение I содержит определения и специальные примечания, значимые для раскрытия уязвимостей и реагирования на киберинциденты. Их применимость устанавливается по конкретной позиции и содержанию передачи. Нельзя превращать исключение для определённой технологии или деятельности в общее освобождение всех продуктов, продаваемых под названием cybersecurity. [1]

Рекомендация Комиссии 2021/1700 посвящена внутренним программам соблюдения правил в исследованиях, связанных с продукцией двойного назначения. Для университета или лаборатории полезны ранняя классификация проекта, распределение ответственности и оценка международного обмена материалами. Однако академическая аффилиация не определяет автоматически, что любая передача является фундаментальным исследованием или общедоступной информацией. Существенны содержание и применимые определения. [14]

Практическая процедура для исследовательского проекта должна быть достаточно быстрой, чтобы не блокировать ответственное устранение уязвимости. ARGА предлагает заранее определить контактное лицо, состав минимального описания и путь срочной правовой оценки. Исследователь сообщает цель и характер передаваемого материала, не раскрывая опасные подробности широкому кругу сотрудников. Решение фиксирует конкретное основание допустимости, а не общее доверие к профессии отправителя.

Защита данных остаётся самостоятельным направлением. Передача продукта и передача персональных данных могут происходить одновременно, но одна авторизация не заменяет другую. В частности, при применимости GDPR необходимо оценивать правовое основание обработки, цели, минимизацию, безопасность и условия международной передачи. Настоящий доклад не предполагает, что Регламент 2021/821 предоставляет самостоятельное разрешение собирать сведения об объектах наблюдения для корпоративного аудита. [15]

Проверка законности не должна сама увеличивать вред. Вместо передачи полного массива наблюдений можно использовать ограниченные журналы администрирования, выборочное независимое подтверждение или обезличенные показатели, если они действительно отвечают на вопрос. Если обезличивание неустойчиво и позволяет восстановить личность, его нельзя считать достаточной защитой. Контроль оценивается по получаемому доказательству, а не по объёму изъятых данных.

Описание уязвимости для исправления следует отличать от передачи более широкого эксплуатационного пакета. Их квалификация может различаться, хотя материалы возникли в одном исследовании. Анализ отдельных частей с последующей оценкой всего пакета помогает одновременно сохранить законный обмен и не пропустить контролируруемую передачу.

18. Шесть практических ситуаций

Ситуация 1. Обычная сетевая диагностика

Европейский поставщик продаёт оператору связи систему измерения нагрузки без функций скрытого наблюдения за людьми. Инженерная проверка подтверждает заявленную конфигурацию; сведений о другом назначении нет. Проверяется приложение I, поскольку сетевой продукт может подпадать под отдельную позицию по своим характеристикам. Если оснований не обнаружено, само слово «мониторинг» не делает его средством кибернаблюдения по статье 2(20).

Решение документирует границы: получатель получает именно диагностический модуль, дополнительные функции не активируются. Если позднее появляется заказ на индивидуальное профилирование, он оценивается отдельно. Практический урок - отрицательный вывод должен быть технически обоснованным и ограниченным проверенной конфигурацией. Он не превращается в бессрочный сертификат для всей линейки продуктов.

Ситуация 2. Неустановленный государственный оператор

Посредник заказывает систему, объективно предназначенную для скрытого наблюдения, но отказывается назвать государственное подразделение, которое будет ею пользоваться. Его регистрация и финансовое положение подтверждены. Эти сведения не закрывают вопрос о конечном использовании. Поставщик запрашивает минимальное подтверждение оператора и правовых оснований, предлагает конфиденциальный маршрут представления данных компетентному органу.

До разрешения существенного противоречия передача внутренне приостанавливается. Отказ раскрыть пользователя не следует автоматически описывать как уже доказанное нарушение статьи 5(2). Однако компания может не располагать достаточным основанием для положительного решения. Если имеются дополнительные факты о предполагаемом репрессивном использовании, оценивается обязанность уведомления и применимое национальное правило о подозрении.

Ситуация 3. Смена страны удалённой активации

Разрешённый проект предусматривает доступ определённого пользователя в одной стране. Перед вводом в эксплуатацию интегратор просит активировать тот же модуль для иной организации в другом государстве. Физический сервер остаётся на прежнем месте. Это не позволяет считать изменение несущественным: карта получателей и доступов больше не соответствует исходному досье.

Поставщик устанавливает, какая передача произойдёт, кто станет экспортёром и охватывает ли её разрешение. До выяснения дополнительный доступ не выдаётся. Если новая организация лишь оказывает техническую услугу без получения контролируемого объекта, этот вывод подтверждается схемой прав. Практический урок - местонахождение оборудования не заменяет анализа получателя программного обеспечения и технологии.

Ситуация 4. Сообщение о преследовании журналиста

Исследователь передаёт технически правдоподобные материалы о применении продукта против журналиста. Они подтверждают вероятную связь с семейством инструментов, но пока не устанавливают оператора. Компания сохраняет материалы, защищает личность заявителя, проверяет версии и сопоставляет их с законно доступными сведениями о поставках. Публичное обвинение конкретного клиента преждевременно.

Если тому же потенциальному оператору предстоит расширение функциональности, вопрос немедленно передаётся ответственному руководителю. Возможна временная остановка расширения с последующей проверкой. Нельзя требовать окончательного судебного решения как единственного основания для профилактического действия. Равным образом нельзя представлять первоначальную техническую гипотезу как доказанную ответственность конкретного лица.

Ситуация 5. Университет и раскрытие уязвимости

Лаборатория планирует передать зарубежному разработчику сведения для исправления обнаруженной уязвимости. Проверка устанавливает содержание материалов, получателя и применимость конкретных определений или примечаний приложения I. Если имеется релевантное исключение, решение ссылается именно на него. Академический статус и общественно полезная цель сами по себе не заменяют правовой анализ.

Если пакет одновременно включает иной контролируемый модуль, его оценивают отдельно. Процедура должна позволять законно передать допустимую часть без необоснованного распространения освобождения на весь пакет. Практический урок - точная предметная квалификация защищает исследование лучше, чем два крайних подхода: безусловный запрет международного обмена и предположение, что наука всегда освобождена от контроля.

Ситуация 6. Разрешение есть, участник изменился

Поставщик получил европейскую лицензию, но перед очередной передачей выявляет существенное изменение статуса участника по применимому ограничительному режиму. Коммерческая команда предлагает использовать старый номер лицензии. Ответственный специалист проверяет актуальный запрет, его персональный и предметный охват, исключения и необходимость отдельного разрешения.

Сам факт исторической санкционной публикации не даёт ответа о текущем статусе; необходима проверка действующей нормы и записи. Если самостоятельный запрет применим, европейская лицензия на продукцию двойного назначения его не снимает. Практический урок - разрешительный документ действует внутри своего режима и не является общей гарантией законности всех элементов сделки.

19. Внутренняя программа и распределение ответственности

Рекомендация 2019/1318 описывает основные элементы внутренней программы соблюдения правил экспортного контроля: участие руководства, организационные ресурсы, обучение, проверку операций, аудит, документацию и безопасность. Она была принята в рамках предшествующего Регламента 428/2009, поэтому используется здесь как организационный ориентир вместе с действующим правом, а не как замена Регламенту 2021/821. [16]

В небольшой компании несколько функций могут выполняться одним сотрудником, но конфликт интересов должен быть управляемым. Продавец не должен единолично закрывать существенное противоречие в собственном контракте. Руководитель принимает остаточный коммерческий риск в пределах закона; он не вправе отменить обязательное разрешение. Правовая команда определяет требования, инженерная - характеристики, операционная - фактическое исполнение. У каждого решения должен быть конкретный владелец.

Обучение строится по рабочим ситуациям. Продавцу нужно распознать смену конечного пользователя, инженеру - изменение конфигурации, администратору - выдачу нового доступа, финансисту - несоответствие плательщика и договора. Универсальная лекция о санкциях не обеспечивает этих навыков. Внутренний канал консультации должен давать своевременный ответ, иначе сотрудники начнут обходить систему из-за её непригодности для обычного рабочего процесса.

Аудит проверяет выборку завершённых операций: совпадение разрешения и поставки, полноту существенных сведений, обработку изменений и исполнение ограничений. Полезен также разбор предотвращённых ошибок. Цель - установить, почему контроль сработал или не сработал, а не увеличить число форм. При обнаружении системного недостатка исправляется процесс, а не только отдельная карточка клиента.

ARGA предлагает оценивать программу по доле операций с установленным конечным пользователем, своевременности классификации новых версий, качеству закрытия вопросов и исполнению корректирующих мер. Число отказов само по себе не является показателем успеха: оно может отражать как внимательный контроль, так и плохо настроенный процесс. Аналогично отсутствие жалоб не доказывает отсутствие вреда, если пострадавшие не знают о канале обращения или не доверяют ему.

Программа должна сохранять знания при смене сотрудников. Обоснование классификации, переписка с органом и пределы прежнего согласования доступны преемникам с соответствующими правами. Иначе неформальные знания исчезают, а старые разрешения начинают восприниматься как бессрочные. Актуальная запись надёжнее воспоминаний бывшего сотрудника.

20. Протокол решения по конкретной поставке

Решение об экспорте должно связывать правовую оценку с разрешением фактического действия. Для этого ARGA предлагает краткий протокол, который сопровождает техническое и правовое досье. Он не заменяет лицензию и не является обязательной государственной формой. Его задача - дать исполнителю точный ответ: какой объект, какому получателю и при каких условиях можно передать сейчас.

В начале протокола фиксируются идентификатор сделки, юридическое лицо экспортёра, версия продукта и планируемое действие. Затем указываются применимые основания контроля, полученные разрешения и вывод по конечному использованию. Важна формулировка предмета: «поставка программного модуля версии 4.2 указанному оператору» проверяема; «работа с клиентом одобрена» слишком широка. Номер версии в этом примере условный и не относится к реальному продукту.

Положительное решение должно содержать пределы и условия. Например, доступ предоставляется только установленному получателю; дополнительная функция не входит в согласованный объём; изменение оператора требует повторного рассмотрения. Если передача разрешается после исполнения условия, система выдачи доступа не должна считать само наличие протокола достаточным. Ответственный подтверждает выполнение условия отдельной записью, связанной с реальной операцией.

Отрицательное решение также требует точного основания. Прямой запрет, отсутствие необходимой лицензии, невозможность установить пользователя и корпоративный отказ из-за остаточного риска – разные причины. Для первых двух вопрос решается в рамках применимого права; для третьей могут помочь дополнительные сведения; для четвёртой нужно определить, допускает ли политика пересмотр. Общее слово «комплаенс» не объясняет ни исполнителю, ни руководству, что делать дальше.

Элемент решения	Пример содержания	Что проверяет исполнитель
Предмет	Определённый модуль и версия	Совпадение передаваемого объекта
Адресат	Юридическое лицо и оператор	Совпадение получателя доступа
Основание	Классификация и применимая авторизация	Действительность и охват
Условия	Ограничение функции или территории	Реальное исполнение ограничения
Срок	Дата или существенное событие пересмотра	Актуальность решения
Ответственный	Лицо с полномочием согласования	Наличие проверяемого одобрения

Рассмотрим условный пример. Поставщик установил пользователя и классифицировал модуль, но заявление заказчика описывает эксплуатацию в одном ведомстве, тогда как схема доступа предусматривает ещё два. Корректный протокол не фиксирует безусловное одобрение всего проекта. Он выделяет несогласованные доступы, запрашивает роль дополнительных ведомств и определяет, можно ли правомерно и технически отделить проверенную часть. Если разделение искусственное и фактически передаёт ту же спорную возможность, частичное одобрение не решает проблему.

После дополнительной проверки возможны разные результаты. Подтверждение исключительно технической роли второго участника способно снять вопрос; установление нового конечного пользователя может потребовать изменения досье и разрешения. Если сведения указывают на предполагаемое использование для репрессий, анализ переходит к статье 5 и соответствующему уведомлению. Протокол сохраняет последовательность изменения фактов, поэтому последующий проверяющий видит, почему первоначальный ответ был пересмотрен.

21. Поэтапная поставка и проверка эффективности мер

Крупные проекты обычно включают демонстрацию, испытание, поставку, обучение и последующие обновления. Не каждый этап имеет одинаковую квалификацию и одинаковый риск. ARGA предлагает оценивать передаваемую возможность на каждом этапе и связывать переход к следующему с необходимыми условиями. Это организационный подход, а не способ разбить контролируруемую операцию на формально незначительные части.

Для испытания можно ограничить набор данных, число операторов и доступные функции, если такие ограничения технически реальны и соответствуют цели. Но слово «пилот» не создаёт освобождения от лицензирования. Если участник получает контролируемое программное обеспечение или технологию, применимое требование оценивается до передачи. Демонстрация на искусственных данных может уменьшить риск для людей, не меняя автоматически экспортную классификацию самого объекта.

Переход к эксплуатации требует сверки с исходным досье. Проверяется, не изменились ли пользователь, место доступа и конфигурация после испытаний. Практически важно отделять принятие продукта заказчиком от юридического согласования поставки. Подписанный акт успешных испытаний подтверждает технический результат, но не заменяет экспортное разрешение и не доказывает законность предполагаемого наблюдения.

Для каждой меры снижения риска следует определить проверяемый результат. Если обещано разделение полномочий, проверяется отсутствие у одного оператора запрещённой совокупности прав. Если ограничена передача третьим лицам, проверяются порядок выдачи новых учётных записей и договорная цепочка. Если предусмотрен независимый аудит, заранее устанавливаются его предмет, доступные доказательства и порядок реакции на выводы. Одна отметка о проведении аудита не показывает, что риск действительно уменьшился.

При оценке затрат следует сравнивать реалистичные альтернативы. Отказ от спорного модуля, изменение архитектуры и отказ от всей сделки имеют разный коммерческий и правозащитный эффект. Предложенная замена должна решать выявленную проблему: более дорогой продукт с той же неконтролируемой возможностью не является мерой снижения риска. Экономическое сравнение помогает выбрать исполнимое решение, но не допускает обмена обязательного запрета на высокую прибыль.

Закрытие проекта также требует внимания. Истечение договора не всегда прекращает доступ, удаляет ключи или устраняет возможность получать обновления. Компания проверяет прекращение тех прав, которые она обязалась или вправе прекратить, сохраняет необходимые записи и оценивает остающиеся обязательства по безопасности. Не следует обещать удаление всех копий у автономного пользователя, если поставщик не может это проверить. Честное описание остаточных возможностей необходимо для оценки последующих обращений и новых договоров.

22. Позиция ARGА и программа внедрения

Позиция ARGА состоит в поддержке адресного контроля, который способен предотвращать тяжёлые злоупотребления и сохранять правовую определённость для добросовестной деятельности. Для этого необходимо последовательно разделять техническую классификацию, фактический риск и юридическое основание ограничения. Расширение перечня без улучшения исполнения не решает проблему посредников и обновлений. Корпоративная проверка без понятного доступа к компетентному органу также оставляет существенную неопределённость.

ARGА предлагает публиковать больше обезличенных разъяснений по пограничным конфигурациям, различая обязательные нормы и рекомендуемые меры. Это помогло бы уменьшить необоснованные различия практики без раскрытия чувствительных сведений о пользователях. Публичная отчётность должна пояснять, что именно считается заявлением, разрешением, отказом и фактическим экспортом. Стоимость выданных лицензий не равна стоимости осуществлённых поставок, а число ограничений не измеряет непосредственно предотвращённый вред.

На уровне компании первые тридцать дней целесообразно посвятить инвентаризации продуктов, версий, каналов доступа и ответственных. Следующий этап - проверка наиболее рискованных действующих отношений, обновлению договорных механизмов и внедрению процедуры обращения к органу. В течение третьего месяца проводится выборочный аудит фактических передач и учебный разбор сообщения о злоупотреблении. Это предлагаемая последовательность, а не установленный законом девяностодневный срок.

Приоритет определяется возможной тяжестью последствий и близостью следующей передачи. Начать с красивой политики, оставив завтра запланированную активацию непроверенной, означало бы неверно распределить ресурсы. Для каждого выявленного разрыва назначаются ответственный, срок и проверяемый результат. Завершением считается изменение фактического процесса: доступ выдаётся после согласования, новая версия классифицируется, а существенный сигнал получает решение.

Система остаётся работоспособной, когда допускает пересмотр и исправление. Добросовестный экспортёр должен иметь возможность доказать, что риск устранён или первоначальная информация оказалась ошибочной. Пострадавший должен иметь безопасный способ сообщить о вреде. Регулятор должен получать достаточные сведения для самостоятельного решения. Эти три условия дополняют друг друга: устойчивый контроль требует и действенных ограничений, и проверяемой процедуры их применения.

Итоговый практический стандарт ARGА - способность ответить на пять вопросов: какая возможность передана, кому она передана, почему операция допустима, какие факты изменяют решение и как организация узнает об этих фактах. Если ответы подтверждены документами и связаны с реальным исполнением, экспортный контроль становится инструментом предотвращения вреда. Если они существуют только в декларации, даже формально полное лицензионное досье оставляет главную проблему нерешённой.

Источники и справочный аппарат

Нормативные акты, официальные разъяснения и судебные материалы. Дата обращения: 28 сентября 2026 года. Номера в квадратных скобках отсылают к списку ниже. Исторические меры не заменяют проверки действующих ограничений на дату конкретной операции.

- [1] Regulation (EU) 2021/821, 20 May 2021. Articles 2-5, 6-11, 15, 27; Annexes I and IV.
<https://eur-lex.europa.eu/eli/reg/2021/821/oj>
- [2] Commission Recommendation (EU) 2024/2659, 11 October 2024. Guidelines on the export of cyber-surveillance items under Article 5; Annex, sections 1-4. <https://eur-lex.europa.eu/eli/reco/2024/2659/oj>
- [3] Commission Delegated Regulation (EU) 2025/2003, 8 September 2025. Amendment of Annex I to Regulation 2021/821. https://eur-lex.europa.eu/eli/reg_del/2025/2003/oj
- [4] Commission Delegated Regulation (EU) 2026/1405, 26 June 2026. Corrections to certain language versions of Regulation 2021/821. https://eur-lex.europa.eu/eli/reg_del/2026/1405/oj
- [5] Direction générale des Entreprises. Service des biens à double usage (SBDU).
<https://www.entreprises.gouv.fr/service-des-biens-double-usage-sbdu>
- [6] Direction générale des Entreprises. Ai-je besoin d'une autorisation auprès du SBDU ? <https://www.entreprises.gouv.fr/espace-entreprises/s-informer-sur-la-reglementation/ai-je-besoin-dune-autorisation-aupres-du-sbdu>
- [7] Direction générale des Entreprises. Obtention d'une licence biens à double usage : qui fait la demande ? Quand faire la demande ? <https://www.entreprises.gouv.fr/espace-entreprises/realiser-mes-demarches/exporter-des-biens-double-usage/obtention-dune-licence>
- [8] ANSSI. Contrôle export. Regulatory guidance on cryptography and dual-use export controls. <https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/controles-reglementaires-cryptographie/controle-export/>
- [9] OHCHR. Guiding Principles on Business and Human Rights. 2011. Principles 17-22 and 29-31.
https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
- [10] BIS. Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. November 2021. Historical administrative action. <https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities>
- [11] US Department of the Treasury. Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium. 5 March 2024. Historical administrative action.
<https://home.treasury.gov/news/press-releases/jy2155>
- [12] European Parliament. Spyware: MEPs call for full investigations and safeguards to prevent abuse. 15 June 2023. Institutional account of the PEGA recommendations. <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse>
- [13] ECtHR, Grand Chamber. Big Brother Watch and Others v. the United Kingdom. Applications 58170/13, 62322/14 and 24960/15. Judgment, 25 May 2021; especially paragraphs 350-364, 377-382 and 448-450.
<https://hudoc.echr.coe.int/eng?i=001-210077>
- [14] Commission Recommendation (EU) 2021/1700, 15 September 2021. Internal compliance programmes for controls of research involving dual-use items. <https://eur-lex.europa.eu/eli/reco/2021/1700/oj>
- [15] Regulation (EU) 2016/679 (GDPR). Articles 5, 6, 25, 32 and Chapter V, subject to its scope of application. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [16] Commission Recommendation (EU) 2019/1318, 30 July 2019. Internal compliance programmes for dual-use trade controls under Regulation 428/2009. Organisational guidance read alongside current law.
<https://eur-lex.europa.eu/eli/reco/2019/1318/oj>