GUIDES TO GOOD GOVERNANCE

No. 06

Балансирование открытости и конфиденциальности в оборонном секторе: уроки международной передовой практики

Centre for Integrity in the Defence Sector
Міністерство оборони України
Norwegian Ministry of Defence

ЦЕНТР ПО УКРЕПЛЕНИЮ ЭТИЧЕСКИХ ОСНОВ В ОБОРОННОМ СЕКТОРЕ

Центр по укреплению этических основ в оборонном секторе (ЦУЭООС) содействует развитию этичности, мер по борьбе с коррупцией и надлежащего управления в оборонном секторе. В сотрудничестве с норвежскими и международными партнерами Центр стремится к наращиванию компетентности, повышению осведомленности и предоставлению практических средств для снижения рисков коррупции. ЦУЭООС был создан Министерством обороны Норвегии в 2012 г.

ОБ АВТОРЕ

Франсиско Кардона (Francisco Cardona) является ассоциированным международным экспертом в ЦУЭООС. Кардона – признанный специалист в сфере разработки и оценки реформ государственной службы и государственного управления, административного права и правосудия, антикоррупционной политики и институционального развития. Его профессиональный опыт включает работу как в родной Испании, где он развивал карьеру в государственной службе, так и в международных организациях, таких как ОЭСР, Программа SIGMA, в которых на протяжении 15 лет он работал в качестве старшего политического аналитика в области государственного управления. В SIGMA он консультировал около 25 стран с переходной и развивающейся экономикой в Восточной Европе, Африке, Латинской Америке и Карибском регионе. Он получил юридическое образование (Университет Валенсии, 1976 г.) и имеет несколько степеней магистра в области государственного управления.

ПРЕДИСЛОВИЕ

Целью «Руководств по надлежащему управлению» ЦУЭООС является представление для широкой аудитории ключевых вопросов в сфере надлежащего управления в краткой и доступной для понимания форме. Руководства имеют лаконичную форму, но в то же время не слишком упрощают представленный в них материал.

В шестом Руководстве по надлежащему управлению автор стремится дать критический анализ понятию конфиденциальности в оборонном секторе. При этом автор задается вопросом: «(...) где должен быть баланс между свободным доступом к информации и ограничением этого доступа в некоторой степени» в демократическом обществе с (...) «открытым правительством»? Кроме того, когда необходимо ограничивать информацию в интересах национальной безопасности? Рассматривается право граждан на государственную защиту.

Руководство написано Франциско Кардона, старшим международным экспертом ЦУЭООС. Я хотел бы поблагодарить его за вклад в такую важную тему в области надлежащего управления. Эта тема была актуальна для общественного обсуждения в последние годы, и, вероятно, останется по-прежнему актуальной в ближайшем будущем.

Я также хотел бы поблагодарить редактора центра Бьорда Бредрупа Кнутсена и нашего координатора публикаций Осе Мари Фоссум за их вклад в руководство.

Мы надеемся, что это руководство будет использоваться широкой аудиторией, как в государственном секторе, включая оборону, так и за его пределами. Сбалансированность открытости и конфиденциальности крайне важна для хорошо функционирующего демократического общества.

ЦУЭООС с благодарностью примет к сведению любые комментарии по поводу данного руководства.

Осло, 24 апреля 2018 г.

Пер Кристенсен

Директор

СОДЕРЖАНИЕ

ВСТУПЛЕНИЕ 3

КОНЦЕПТУАЛЬНАЯ БАЗА: НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ КАК ОБОСНОВАНИЕ ДЛЯ КОНФИДЕНЦИАЛЬНОСТИ 4

Слабая общая роль судебных органов в процессе контроля систем секретности 8

Критерии и уровни секретности 9

Критерии для снятия грифа секретности 12

Применение тестов для контроля секретности: тест на возможный вред и тест балансирования общественного интереса 13

ИТОГИ 16

СПИСОК ЛИТЕРАТУРЫ 18

Вступление

В настоящем руководстве по надлежащему управлению представлен краткий обзор передовых международных практик стран ЕС и ОЭСР, направленных на сохранение конфиденциальности общественной информации в области обороны и национальной безопасности и в то же время на продвижение общего права общественности на доступ к информации, находящейся в распоряжении государственных учреждений. Целью данного руководства является представление политик, продвигающих идеи открытого правительства, доступа к информации и способности граждан принимать обоснованные решения касательно деятельности правительства. В то же время, дается определение границ для правильной защиты государственной тайны в вопросах, касающихся национальной безопасности, обороны и разведки, а также борьбы с коррупцией и преступностью.

Прозрачность и гласность являются отличными профилактическими средствами против коррупции, недобросовестного администрирования и плохого управления. Демократии не могут работать должным образом в условиях секретности, так как если секретность преобладает, то политический режим просто становится недемократичным, поскольку его граждане исключены из политического процесса. Это приводит к тому, что процесс осуществления власти может выйти из-под контроля, а демократическая подотчетность не может быть реализована. Однако, общественный доступ к информации также может быть ограничен, чтобы сохранить надлежащее функционирование демократии в эффективно управляемом государстве. Следовательно, как раскрытие публичной информации, так и некоторые ограничения такого раскрытия должны одинаково служить на благо общественных интересов.

Концептуальная база: национальная безопасность как обоснование для конфиденциальности

Основное концептуальное предположение заключается в том, что открытое правительство и свободный доступ к информации, с одной стороны, и ограничение этого доступа в некоторой степени, с другой стороны, служат на благо интересов общества. Общепризнанный международный принцип заключается в том, что «право знать» должно поощряться правительством, в то же время следует устанавливать разумные ограничения для защиты конфиденциальности определенной публичной информации. Последнее необходимо для того, чтобы деятельность государства в определенных областях, особенно в тех, которые связаны с национальной безопасностью и обороной, осуществлялась эффективно.

Основная проблема в отношении такой секретности состоит в том, чтобы определить, когда и в какой степени ограничения общественного доступа к информации являются оправданными. Амбициозная цель здоровых демократий – обеспечить надлежащий доступ общественности к информации, одновременно устанавливая определенные законные границы для ограничения этого доступа. Установление правильного баланса между этими двумя аспектами очень сильно зависит от истории страны, общественных ценностей и других культурных факторов. По этой причине трудно определить, существуют ли международные стандарты, помогающие достичь правильного баланса (Трансперенси Интернешнл Великобритания, 2014 г.). На практике точных международных стандартов не существует, хотя в последние годы было много интеллектуальных дискуссий и попыток установить некоторые общие принципы.[1]

Практика обеспечения секретности и конфиденциальности, если ее оставить без контроля, легко становится довольно значительной и обширной. Некоторые государственные службы, занимающиеся вопросами национальной безопасности, обороны, уголовных расследований, сбора разведывательных данных или борьбы с терроризмом, имеют тенденцию применять секретность ко всему, что они делают, даже если это приводит к тому, что граждане лишаются права знать то, чем занимается правительство. Помимо высокой стоимости поддержания «механизма секретности», существенное и широкое

1 См. Принципы Цване (2013 г.). Доступно по адресу: https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

использование конфиденциальности имеет тенденцию подрывать доверие общественности к государственным институтам власти и, в конечном итоге, ослаблять демократическую легитимность. Слишком высокий уровень секретности также приводит к большему количеству ошибок и правонарушений, чем прозрачность и общественный контроль, так как отсутствие прозрачности затрудняет общественный контроль и корректирование неправильных практик. В результате в долгосрочной перспективе чрезмерная секретность может угрожать национальной безопасности больше, чем открытость.

Как утверждают некоторые государственные чиновники – например, в Соединенных Штатах – слишком большая секретность «стала неоправданным препятствием для обмена информацией внутри и за пределами правительства, в ущерб государственной политике» (Афтергуд, 2008 г., стр. 400). Это указывает на проблему чрезмерной секретности, то есть на то, что службы хранения информации имеют тенденцию засекречивать информацию в той степени, которая намного превышает фактическую необходимость.

Целью любой системы секретности является предотвращение разглашения информации, которая может поставить под угрозу национальную безопасность, но неопределенность таких понятий как «национальная безопасность» и «угроза безопасности» легко создает условия для чрезмерного использования секретности. Трудность установления различия между фактической и субъективной информацией затрудняет установление четко определенных критериев правильной секретности данных.

Правильная секретность информации сама по себе является очень сложным понятием, но концептуально мы можем согласиться с тем, что «разумная» секретность это та, которая является обоснованной и как можно меньше отходит от демократических ценностей открытости, прозрачности и свободного доступа к информации. Другими словами, мы можем согласиться с тем, что разумным ограничением прозрачности является то, что а) является исключительным и б) защищает важные интересы национальной безопасности. В этом заключении признается наличие информации в области обороны и национальной безопасности, сокрытие которой *не является* критическим для национальной безопасности и, следовательно, может быть безопасно раскрыто – полностью или частично.

В некоторых демократических странах все еще преобладает традиционный подход, согласно которому прозрачность просто представляет потребность гражданина, а секретность ради национальной безопасности представляет общественный интерес. Например, г-н Жан Марк Сове, заместитель председателя Государственного совета Франции, сказал в своем обращении к Национальной ассамблее Франции, нижней палате французского парламента, 5 июля 2011 года: *«Это путь вперед в очерчивании разделительной линии между легитимными государственными интересами, претендующими на секретность, и прозрачностью, которой требуют граждане»* (Сове, 2011 г., стр. 6). Это заявление основывается на предположении, что сохранение секретности защищает общественный интерес, тогда как прозрачность не является общественным интересом, а лишь

запросом, вызванным любопытством граждан и журналистов. Это очень сомнительное предположение. Опыт показывает, что продвижение прозрачности является одним из лучших способов защиты общественных интересов, поскольку это способствует тому, чтобы государственные органы были подотчетны гражданам и другим механизмам демократического контроля. Поэтому именно прозрачность, а не секретность, можно рассматривать как средство *преодоления* «разрыва, который естественным образом возникает между государством и общественностью» (Фенстер, 2010 г., стр. 619).

Существует широкий международный консенсус в отношении того, что прозрачность в политике и действиях государственных органов должна быть общим правилом, тогда как секретность должна быть исключением. Более того, такие исключения должны быть обоснованными: они могут быть оправданы, только если они легитимны. Такие исключения являются легитимными только в том случае, если может быть доказана их необходимость для защиты подлинных интересов национальной безопасности.

Необходимость различать легитимную и нелегитимную секретность требует определенного контроля со стороны органов власти, не зависящих от органа, применяющего секретность. Такие независимые механизмы контроля могут осуществляться судами или более специализированными государственными органами, и их роль заключается в установлении того, являются ли интересы национальной безопасности, на которые ссылаются органы, удерживающие информацию в тайне, подлинными и достаточно важными для этого. Без механизмов внешнего контроля решения о присвоении секретности информации становятся исключительно дискреционными и, скорее всего, произвольными. Однако, как мы увидим далее, исторически суды играли такую роль, и все еще склонны ее исполнять, которая чрезмерно благосклонна к сокрытию информации службами безопасности или разведывательными органами.

Концептуально полная прозрачность нежелательна и, вероятно, невозможна, как указано выше. Кроме того, у государства всегда есть деятельность в определенных областях, которые являются неясными или неоднозначными. Как указывает Фенстер (2010 г., стр. 623), часто существует область между секретностью и прозрачностью, которая означает, что секретность не обязательно является полной противоположностью прозрачности. На практике секретность и прозрачность не представляют собой четко противоположные реальности, так как и секретность, и прозрачность требуют отдельных институционных основ, которые структурно отличаются (Риз, 2014 г., стр. 14).

Большая прозрачность не обязательно означает меньшую секретность, но лучшее ее качество обеспечит защиту конфиденциальности. Большая прозрачность означает, что будут защищены только подлинные потребности в конфиденциальности. Институционализация политик прозрачности является относительно новым процессом в большинстве стран, тогда как институционализация секретности происходит из давно установленных традиций. Ценности и интересы каждой из этих традиций по-прежнему неоднородны и в какой-то мере противоречивы.

Задача состоит в том, чтобы постепенно сделать институционализацию права на получение информации и защиту подлинных потребностей в конфиденциальности более гармонизированными – в организационных структурах, которые имеют дело с ними, и в правительственных практиках. Поиск большей согласованности между двумя политиками в идеале должен способствовать формированию единой, интегрированной политики и более последовательной институционализации доступа к информационной политике в национальных правительствах в соответствии с потребностями национальной безопасности.

Однако, понятие «национальная безопасность» весьма неясно, поскольку оно может означать разные вещи в разных национальных контекстах, что еще больше усложняет проблему. В большинстве европейских стран, изученных Якобсен (2013 г.), национальная безопасность в той или иной степени охватывает международные отношения, а также угрозы внутренней безопасности. Другими словами, здесь не обязательно существует очевидная граница.

Чтобы установить, является ли государственная тайна законной, Афтергуд (2009 г., стр. 402-403) предлагает три практические категории секретности, признавая при этом, что неизменная проблема государственной политики заключается в том, чтобы отделить легитимную тайну от нелегитимной и сохранить первую, раскрывая последнюю:

1. **Подлинная секретность национальной безопасности:** применяется для защиты информации, которая может представлять определенную угрозу безопасности нации, ставя под угрозу ее оборону или реализацию международных отношений. Удерживание такой информации в тайне не вызывает споров, потому что это является обоснованием всех систем секретности, и государственный интерес обеспечивается лучше всего в том случае, когда этот тип информации остается секретным.

2. **Бюрократическая секретность:** является склонностью бюрократов защищать информацию, будь то по соображениям удобства или при наличии некоторого подозрения, что ее разглашение может быть более рискованным, чем удержание в тайне. Эта бюрократическая тенденция обычно приводит к чрезмерной секретности информации и к излишне большому количеству засекреченной информации. Это также увеличивает бюджетные расходы на секретность и часто играет на бюрократическом чувстве собственной значимости и нежелании показывать то, как конкретное государственное учреждение выполняет свою работу.

3. **Политическая секретность:** тенденция использования секретности для обеспечения политических преимуществ. Эта форма секретности является наиболее спорной и нежелательной, поскольку она использует общепризнанную законность подлинных интересов национальной безопасности в целях продвижения корыстных программ, избегания политических противоречий или нарушения государственной подотчетности. В крайних случаях политическая тайна скрывает нарушения закона, нарушения прав человека, коррупцию или злоупотребления и угрожает целостности политического процесса.

СЛАБАЯ ОБЩАЯ РОЛЬ СУДЕБНЫХ ОРГАНОВ В ПРОЦЕССЕ КОНТРОЛЯ СИСТЕМ СЕКРЕТНОСТИ

Как указывалось ранее, суды традиционно проявляли, и до сих пор демонстрируют, весьма почтительное отношение в своих реакциях на действия органов, засекречивающих данные, и их так называемую «*исполнительную привилегию в вопросах государственной тайны*». Такое уважительное отношение представителей судебной власти помогло закрепить идею о том, что вопросы национальной безопасности являются слишком чувствительными, чтобы их можно было раскрывать даже в судах (Сетти, 2012 г.). Хорошим примером из истории США является знаковое дело, случившееся во время холодной войны, известное как «*Соединенные Штаты против Рейнольдса*».[2]

Почтительное расположение судов к исполнительной власти усилилась после террористических атак в США 11 сентября, которые часто называют «9/11» – 11 сентября. Заявления правительства о защите национальной безопасности в ходе судебных процессов неизменно преобладали над такими принципами как подотчетность, прозрачность и открытое правительство. Многие случаи в США, Великобритании, Франции и других странах демократического мира, не говоря уже о менее демократических странах, отражают лежащую в основе приверженность узкому взгляду на роль судебных органов в отношении пересмотра исполнительных решений, связанных с вопросами безопасности. К сожалению, это может нанести ущерб защите фундаментальных прав, верховенству закона и соблюдению подлинных интересов безопасности.

«*Исполнительная привилегия в вопросах государственной тайны*» в США или «*сертификат об иммунитете государственных интересов*» в Великобритании или «*оборонная секретность*» во Франции, очень часто применяются исполнительными органами, имеющими дело с секретностью, с целью предотвращения судебного рассмотрения, либо для того, чтобы сделать его менее эффективным. Исключения соблюдения открытости данных, основанные на утверждениях, подобных трем вышеупомянутым терминам, регулярно принимаются судами, даже если – иногда – суды неотчетливо заявляют, что эта привилегия должна быть ограничена только случаями подлинной национальной безопасности. Эта довольно распространенная судебная позиция, как правило, выявляет «неуважительное отношение судов к понятию сдержек и противовесов, отказ от судебной ответственности и пренебрежение структурной необходимостью сохранить возможность для истцов обращаться за возмещением ущерба в случае чрезмерных действий правительства» (Сетти, 2012 г., стр. 1573).

Фукс (2006 г., стр. 168) в своем выдающемся исследовании роли судов обнаружила, что «учитывая значимые ценности, обусловленные правом на доступ к правительственной информации, этим правом следует жертвовать только тогда, когда существует законная потребность в секретности… Ни парламенты, ни общественность сама по себе не в состоянии оспаривать чрезмерную секретность. Независимая проверка является частью ответственности судебной власти для

2 Доступно по адресу: https://supreme.justia.com/cases/federal/us/345/1/case.html

обеспечения надлежащего санкционирования действий правительства». Только суды имеют достаточную независимость, чтобы исполнять роль оспаривателя чрезмерной секретности, но, по-видимому, как отмечает Фукс, они отказались взять на себя эту роль.

Почти во всех европейских странах, изученных Якобсен (2013 г.), суды имеют полномочия для доступа к секретной информации, которую правительство стремится сохранить в тайне исходя из соображений национальной безопасности. Однако, примечательно то, что в некоторых странах только определенные суды или судьи, имеющие специальное разрешение, могут проводить проверку секретной информации. В Германии только Федеральный административный суд может рассматривать секретную информацию. В Испании, хотя закон об официальной тайне и не предусматривает доступ для судей, как это делается для Конгресса и Сената, Верховный суд Испании постановил, что только он в единственном лице имеет право рассматривать секретную информацию, находящуюся в распоряжении правительства. Единственной страной, в которой суды совсем не имеют полномочий напрямую проверять секретную информацию, является Франция (Сартр и Ферле, 2010 г.). Для французского судьи кажется невозможным прямой доступ к изучению секретной информации. Чтобы ограничить действие этого запрета, в соответствии с законом 1998 года, была создана французская Комиссия по вопросам секретности национальной обороны (CSDN), независимая комиссия, которая может получать доступ к секретной информации по запросу судьи, чтобы оценить, является ли разумным рассекречивание этой информации.[3] Что касается ЕС, то в большинстве стран Европы судебные органы обычно полагаются на оценку государственного органа относительно того, что раскрытие информации может нанести ущерб интересам национальной безопасности (Якобсен, 2013 г.).

КРИТЕРИИ И УРОВНИ СЕКРЕТНОСТИ

Уровни секретности были стандартизированы таким образом, что во многих странах ОЭСР можно найти одну и ту же систему классификации. Среди стран ОЭСР хорошим примером того, как осуществляется работа с государственной тайной, является Новая Зеландия. В Новой Зеландии официальная информация защищена в соответствии с критериями, основанными на строгом определении необходимости защиты официальной информации: информация должна быть защищена в той степени, которая соответствует общественным интересам и сохранению конфиденциальности. Секретность информации определяется попытками классифицировать такую информацию исходя из ущерба, который может возникнуть в результате ее несанкционированного разглашения, с уточнением защитных мер, которые должны быть применены.[4] Согласно новозеландским руководящим директивам, секретность сама по себе не обеспечивает сокрытие официальной информации; скорее информация должна рассматриваться по существу в соответствии с критериями, установленными законом.[5] Австралийская

3 Доступно по адресу: https://supreme.justia.com/cases/federal/us/345/1/case.html

4 Закон об официальной информации Новой Зеландии 1982 г.

5 Новозеландские директивы для защиты официальной информации. Доступно по адресу: https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

система определения степени секретности интересна тем, что в ней содержатся четкие указания относительно того, как устанавливать секретность и рассекречивать данные.[6]

Уровни секретности в Новой Зеландии, которые соответствуют широко используемой международной практике, определяются следующим образом, в зависимости от общественного блага, которое необходимо защитить:

- Данные, связанные с национальной безопасностью: раскрытие информации может поставить под угрозу безопасность, оборону или международные отношения страны или дружественных правительств, либо

- Данные, связанные с политикой правительства и/или с конфиденциальностью: раскрытие информации может поставить под угрозу функционирование правительства или причинить убытки человеку.

Информация, связанная с национальной безопасностью, имеет следующие уровни защиты с использованием таких критериев:

1. **Совершенно секретно:** раскрытие данных может нанести особенно тяжелый ущерб национальным интересам:
   - Непосредственно угрожать внутренней стабильности Новой Зеландии или дружественных стран
   - Привести непосредственно к массовой гибели людей
   - Нанести исключительный ущерб безопасности сил Новой Зеландии или союзников
   - Нанести исключительный ущерб оперативной эффективности сил Новой Зеландии или дружественных сил
   - Нанести исключительный ущерб непрерывной эффективности особо ценных операций в сфере безопасности или разведки
   - Нанести исключительный ущерб отношениям с другими правительствами
   - Причинить серьезный долгосрочный ущерб значимой национальной инфраструктуре
2. **Секретно:** раскрытие данных может нанести серьезный ущерб национальным интересам:
   - Привести к международной напряженности
   - Нанести серьезный ущерб отношениям с дружественными правительствами
   - Нанести серьезный ущерб безопасности сил Новой Зеландии или дружественных сил
   - Нанести серьезный ущерб оперативной эффективности сил Новой Зеландии или дружественных сил
   - Нанести серьезный ущерб эффективности ценных операций в сфере безопасности или разведки

6 Австралия (2014 г.): Директивы по управлению безопасностью информации. Система секретности правительства Австралии. Доступно по адресу: https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

- Нанести серьезный ущерб внутренней стабильности Новой Зеландии или дружественных стран
- Привести к закрытию или существенно подорвать деятельность значимой национальной инфраструктуры

3. **Конфиденциально:** раскрытие данных может нанести значительный ущерб национальным интересам:
   - Нанести материальный ущерб дипломатическим отношениям – вызвать официальный протест или другие санкции
   - Нанести ущерб операционной эффективности сил Новой Зеландии или дружественных сил
   - Нанести ущерб безопасности сил Новой Зеландии или дружественных сил
   - Нанести ущерб эффективности ценных операций в сфере безопасности или разведки
   - Нанести ущерб внутренней стабильности Новой Зеландии или дружественных стран
   - Подрывать деятельность значимой национальной инфраструктуры
4. **Для служебного (ограниченного) использования:** раскрытие данных может негативно повлиять на национальные интересы:
   - Негативно влиять на дипломатические отношения
   - Препятствовать оперативной эффективности сил Новой Зеландии или дружественных сил
   - Препятствовать безопасности сил Новой Зеландии или дружественных сил
   - Негативно влиять на внутреннюю стабильность Новой Зеландии или дружественных стран
   - Негативно влиять на экономическое благополучие Новой Зеландии или дружественных стран

Государственная политика и личные данные частных лиц защищаются на следующих уровнях с использованием таких критериев:

1. **Закрытые данные с ограниченным доступом:** их раскрытие может нанести ущерб правопорядку, препятствовать ведению государственных дел, повлиять на неприкосновенность частной жизни граждан:
   - Ставить под угрозу безопасность любого человека
   - Нанести серьезный ущерб экономике Новой Зеландии
   - Препятствовать правительственным переговорам
2. **Данные на конфиденциальной основе:** их раскрытие может нанести ущерб правопорядку, препятствовать ведению государственных дел, повлиять на неприкосновенность частной жизни граждан:
   - Наносить ущерб соблюдению законов

- Неблагоприятно влиять на частную жизнь физического лица
- Наносить ущерб коммерческой информации гражданина
- Наносить ущерб обязательствам о неразглашении конфиденциальной информации
- Наносить ущерб реализации мер по защите здоровья или безопасности граждан
- Наносить ущерб экономическим интересам Новой Зеландии
- Наносить ущерб мерам, которые предотвращают или смягчают материальные потери для общественности
- Приводить к нарушению конституционных конвенций
- Препятствовать эффективному ведению государственных дел
- Приводить к нарушению законных профессиональных привилегий
- Препятствовать правительственной коммерческой деятельности
- Разглашение или использование информации для ненадлежащего получения прибыли или выгоды

Как уже отмечалось, подобные маркировки и критерии секретности информации можно найти во многих странах ОЭСР. Даже в Турции, где правила секретности не являются общедоступными, известно о существовании определенных уровней секретности (Якобсен 2013 г.). Швеция оказалась единственной страной, которая предоставила данные в рамках исследования Якобсен (2013 г.), в которой закон не устанавливает уровни секретности информации, поскольку в Швеции секретность выполняет исключительно административную функцию.

Другие аспекты, связанные с секретностью информации (например, процедуры засекречивания, требования к маркировке, полномочия по секретности, обязательства по обоснованию секретности, ответственность за некорректную секретность, органы надзора и контроля и т. д.), имеют значительные отличия в разных европейских странах (см. Якобсен 2013 г. и Трансперенси Интернешнл Великобритания, 2014 г.).

КРИТЕРИИ ДЛЯ СНЯТИЯ ГРИФА СЕКРЕТНОСТИ

В европейских странах рассекречивание информации определяется тремя основными критериями: временными рамками, событием-триггером или обязательным периодом пересмотра данных. Основная цель в этом вопросе – предотвратить бессрочное засекречивание информации. Тем не менее, нередко можно найти страны, в которых отсутствуют критерии для снятия грифа секретности в законодательстве или административных практиках. Среднее ограничение срока секретности, согласно расчетам Якобсен (2013 г.), для европейских стран составляет 30 лет, с указанием конкретных временных рамок, которые варьируются от 10 лет в Нидерландах до 100 лет в Румынии и до неопределенного срока в Испании и Турции.

Последнее, однако, является скорее исключением в Европе.

Наиболее распространенный период обязательного пересмотра секретной информации составляет 5 лет. В Швеции нет предварительно установленного обязательного пересмотра, но секретность любого вида информации должна пересматриваться всякий раз, когда делается запрос на раскрытие информации. Практика автоматического рассекречивания (событие-триггер) варьируется в зависимости от страны, но в большинстве из них основным аспектом является решение правительства, принятое по его усмотрению, о рассекречивании различных классов информации. Такое решение также может быть следствием исполнения процедуры Закона о доступе к информации, которая осуществляется гражданином или гражданской организацией.

ПРИМЕНЕНИЕ ТЕСТОВ ДЛЯ КОНТРОЛЯ СЕКРЕТНОСТИ: ТЕСТ НА ВОЗМОЖНЫЙ ВРЕД И ТЕСТ БАЛАНСИРОВАНИЯ ОБЩЕСТВЕННОГО ИНТЕРЕСА

Согласно *Right2INFO.org*, общественной организации, пропагандирующей надлежащие законы и практики, так называемый тест на возможный вред (Harm Test) и тест на общественный интерес (Public Interest Test) происходят из требования относительно того, что ограничения права на доступ к информации должны быть пропорциональными и необходимыми.[7] ОЭСР-SIGMA (2010 г.) предлагает содержательный и глубокий концептуальный подход к понятиям, стоящим за этими тестами, исходя из различия между абсолютными и относительными ограничениями в отношении доступа к информации. К первым в основном относятся те, которые относятся к обороне и национальной безопасности.

ТЕСТ НА ВОЗМОЖНЫЙ ВРЕД

В соответствии с тестом на возможный вред, государственный орган должен показать, что раскрытие определенной информации составляет угрозу нанесения ущерба защищенным интересам. Следовательно, раскрытие таких данных не должно произойти. Тест на вред требует, чтобы государство обосновало риск существенного и очевидного ущерба для данного легитимного интереса. Должно быть продемонстрировано, что ограничение связано с определенным легитимным интересом, и что раскрытие информации нанесет существенный ущерб этому интересу. Такой вред должен быть достаточно четко определенным, конкретным, неизбежным и прямым, а не спекулятивным или сомнительным.

ТЕСТ БАЛАНСИРОВАНИЯ ОБЩЕСТВЕННОГО ИНТЕРЕСА

Тест на балансирование общественного интереса ссылается на пропорциональность. Для этого требуется проведение оценки баланса, при которой вред от раскрытия данных оценивается относительно общественного интереса, который удовлетворяется посредством раскрытия. Условия, при которых явный и конкретный общественный интерес может перевесить требования секретности/конфиденциальности, должны быть определены национальным законодательством. Согласно многим национальным моделям секретности, включая межамериканские и афри-

7 Доступно по адресу: http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

канские, общественный интерес становится обязательным и имеет приоритет над другими интересами в том случае, если информация касается нарушений прав человека или преступлений против человечества. Тест на установление баланса требует, чтобы государственный орган или орган контроля взвесили ущерб, который может причинить раскрытие данных определенному защищенному интересу, в противовес общественному интересу, которому служит раскрытие этой информации.

Определение того, что представляет собой общественный интерес, отличается в разных странах и часто требует оценки в каждом конкретном случае. В целом, общественные интересы, способствующие раскрытию информации, обычно включают вопросы публичных дебатов, участия общественности в политических дебатах, подотчетности за распределение и траты государственных средств, а также вопросы общественной безопасности. Вопросы, связанные с общественной безопасностью и окружающей средой, существенными угрозами для здоровья и информация, связанная с грубыми нарушениями прав человека, как правило, рассматриваются как таковые, что оправдывают обязательный приоритет интереса общественности в раскрытии информации.

Некоторые страны выпустили директивы для административных процедур государственных служащих. Например, в Новом Южном Уэльсе, Австралия, при принятии решения о разглашении информации государственные служащие должны применять тест балансирования общественных интересов. Это означает, что они должны сопоставлять факторы в пользу раскрытия относительно факторов общественного интереса против раскрытия.[8] В соответствии с этими рекомендациями, тест балансирования общественных интересов включает три этапа:

1. Определение общественного интереса в пользу раскрытия информации.

2. Определение общественного интереса против раскрытия информации.

3. Определение относительного значения общественного интереса в пользу и против раскрытия и установление того, где находится баланс между этими интересами.

Несмотря на четкую позицию австралийского законодательства в отношении раскрытия информации, провинциальные законы о доступе к информации устанавливают ряд ситуаций, когда презумпция выступает за утаивание информации и защиту секретности. Наиболее выдающейся является информация, которая подпадает под действие закона о секретности, в связи с чем специально определено 26 законных актов. Это соответствует общей тенденции, затрагивающей многие страны ОЭСР, в соответствии с которой законы о свободе информации (FOIA) на практике перестали быть актуальными на пересечении с традиционным законодательством о государственной тайне. Государственные тайны постоянно держатся за рамками законодательства о свободе доступа к информации. Кроме того, в большинстве стран, как правило, было предпринято мало усилий для обеспечения соответствия традиционного законодательства о

8 Доступно по адресу: http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

государственной тайне новому законодательству о свободе доступа к общественной информации.

Тот факт, что многие Законы о свободе информации практически не затронули секретность, связанную с национальной безопасностью, означает, что законодательство и обращение в суды до сих пор оказались недостаточно эффективными инструментами для снижения универсальной тенденции к широкому использованию конфиденциальности и секретности в деятельности органов безопасности и разведки. Такие учреждения, с их традиционным и часто непрозрачным способом обращения с конфиденциальной информацией, в основном остаются незатронутыми законами о свободе информации, несмотря на распространенную международную тенденцию в пользу большей общественной прозрачности и требования гражданского общества исполнения «права знать».

Все это указывает на тот факт, что введение в действие общего законодательства, которое эффективно балансирует секретность и открытость, является сложной задачей как концептуально, так и на практике. Одна из причин этого заключается в том, что государственные органы или агентства, которые чаще всего засекречивают информацию, обычно имеют совершенно разные цели и мотивы в своей работе и практике. Это способствует усилению различных административных культур, связанных с безопасностью. Например, военные органы, как правило, уделяют основное внимание безопасности оружейных технологий и оперативных планов, разведывательные органы – защите источников и методов работы, дипломаты обеспокоены международными последствиями засекречивания и раскрытия дипломатической информации, а полиция стремится защитить своих информаторов и оперативные планы. Это приводит к тому, что каждый орган или ведомство разрабатывают свои собственные руководства, процедуры и протоколы, которые, как правило, остаются в силе в течение многих лет без тщательного анализа и серьезного пересмотра. Кроме того, понятно, что в агентствах, подобных тем, которые перечислены выше, сотрудники предпочитают играть на безопасной территории, чтобы избежать неоправданных проблем, что часто приводит к проявлению чрезмерной секретности (Афтергуд, 2009 г.).

В результате, информированные наблюдатели и практики предполагают, что даже если определённому ведомству необходимо произвести засекречивание, то орган по снятию секретности и раскрытию должен находиться вне этого ведомства. Это лучший способ свести на нет собственные интересы такого ведомства и очистить его от злоупотребления секретностью (Афтергуд, 2009 г., стр. 412). Некоторые успешные попытки реализовать это были предприняты в Соединенных Штатах, например, посредством создания *Межведомственной апелляционной коллегии по вопросам секретности* (ISCAP) [9] и *фундаментального анализа политики секретности* (FCPR).[10] Французская Комиссия по вопросам секретности национальной обороны (CSDN) представляет собой еще один пример (см. выше). Американский опыт, описанный Афтергуд (2009 г.), по сути, показывает, что «если одно агентство не может успеш-

9 Доступно по адресу: http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

10 Доступно по адресу: http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

но объяснить и убедить вышестоящее должностное лицо или коллегию из других ведомств, почему национальная безопасность требует, чтобы определенный элемент был засекречен, то есть причины сомневаться в необходимости сохранения его в тайне вообще».

ИТОГИ

1. Законодательство, регулирующее конфиденциальность информации в области безопасности и обороны, является необходимым и должно быть максимально точным. Такое законодательство должно предусматривать критерии секретности и раскрытия информации, принимая во внимание, что законодательство по определению является общим, и, следовательно, указанные критерии также будут общими. Законодательство, регулирующее конфиденциальность, которое во многих странах превосходит по значимости законодательство о свободном доступе к информации, должно быть согласовано с последним, чтобы предотвратить несоответствия в национальном правопорядке.

2. Наряду с надежной правовой базой, необходимо обеспечить сознательное и профессиональное управление на уровне ведомств для разумного и правильного применения правовых критериев секретности, чтобы в максимальной степени способствовать укреплению демократических ценностей и принципа общественной прозрачности. Осознанное понимание необходимости балансировать различные факторы должно быть частью организационной культуры. Руководители соответствующих учреждений должны рассматривать это как свою задачу в достижении сбалансированного подхода к легитимной конфиденциальности и легитимной прозрачности.

3. Снижение неоправданной чрезмерной секретности и обеспечение баланса между правом на информацию и императивами национальной безопасности – и другими законными причинами секретности – являются сложной задачей. Преобразование культуры секретности в культуру прозрачности в оборонной сфере, вероятно, недостижимо в обозримом будущем в большинстве стран ЕС и ОЭСР.[11]

4. От сотрудников и других лиц, работающих в сфере безопасности и обороны, ожидается лояльность, соблюдение установленных процедур и осмотрительность. Эти качества действительно необходимы, но все же можно и нужно поощрять определенную степень инноваций и новых идей, даже если пространство для изменений может казаться незначительным. Тем не менее, необходимо критически взглянуть на то, как достичь оптимального баланса между легитимной секретностью, с одной стороны, и легитимным доступом к информации, с другой.

11 Даже если кажется, что Румынии это удалось (Матей, 2007 р.).

5. Персонал, отвечающий за реализацию законов о секретности или политик конфиденциальности, должен быть специально обучен, чтобы иметь необходимое согласованное понимание значимости демократической потребности в открытости и прозрачности правительства, и в то же время четко распознавать, что в рамках законодательства необходимо скрывать от взора общественности. Неразборчивое раскрытие данных не является альтернативой беспорядочной секретности. Профессионализм и компетентность сотрудников, работающих в сфере безопасности и обороны, имеют первостепенное значение, поскольку это имеет прямые последствия для демократического общества и отношений между органами безопасности и гражданской общественностью.

6. Независимое учреждение, например, межведомственная комиссия по вопросам снятия секретности и раскрытия, находящееся за пределами исключительной компетенции наиболее важных агентств, применяющих секретность, то есть военных, разведывательных и полицейских органов, должно обладать полномочиями для проверки и периодического рассекречивания информации, которая удерживается в тайне отдельными учреждениями. Судебные органы в целом проявили слишком уважительное отношение к исполнительной привилегии в вопросах государственной тайны, и на данный момент мало оснований для того, чтобы ожидать изменений в этом отношении.

7. Сейчас, похоже, появляются хорошие практики, которые подразумевают сокращение дискреционных практик по сравнению с традиционными подходами к секретности: решение о засекречивании и раскрытии информации должно приниматься не отдельным лицом, а независимым комитетом или комиссией, способной принимать беспристрастные решения о необходимости применения секретности либо раскрытия определенного фрагмента информации – полностью или частично. В своей работе такое специализированное подразделение должно руководствоваться законодательно установленными критериями для определения вреда и проведения оценки баланса интересов. Членство в таком независимом комитете или комиссии должно быть ограничено, например, в него могут входить от 5 до 7 членов, включающих экспертов в области безопасности, представляющих исполнительную власть, парламент, депутатов и омбудсмена, а также судебные органы.

СПИСОК ЛИТЕРАТУРЫ

Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works*," в Yale Law & Policy Review, Том 27, № 2 (весна, 2009 г.), стр. 399-416. Доступно по адресу: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, в Administrative Law Review, стр. 617-672, доступно по адресу: http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play в Preventing Unnecessary Secrecy*, in Administrative Law Review, том 58, №1, зима 2006 г., стр. 131-176.

Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Доступно по адресу: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, в Strategic Insights, том VI, выпуск №3 (май 2007 г.). Доступно по адресу: https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OECP (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*", документы SIGMA, №46, Издательство ОЭСР, Париж. Доступно по адресу: http://dx.doi.org/10.1787/5km4g0zfqt27-en

Riese, Dorothée (2014): *Secrecy and Transparency*, документ был представлен на конференции Европейского консорциума политических исследований в Глазго, 3-6 сентября 2014 г. Доступно по адресу: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

Sartre, Patrice & Ferlet, Philippe (2010): *Le secret de défense en France* in Revue Études 2010/2, том 412, февраль, стр. 165-175. Доступно по адресу: https://www.cairn.info/revue-etudes-2010-2-page-165.htm

Sauvé, Jean-Marc (2011): *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, выступление в Национальной Ассамблее, вторник, 5 июля 2011 г., во время симпозиума, организованного Транспеpенси Интернешнл Франция. Доступно по адресу: http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

Setty, Sudha (2012): *The Rise of National Security Secrets*, in Connecticut Law Review, том 44, №5, июль 2012 г., стр. 1563-1582.

Трансперенси Интернешнл Великобритания (2014 г.): Секретная информация: анализ 15 стран. Доступно по адресу: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

Руководства по надлежащему управлению

GUIDES TO GOOD GOVERN-ANCE
No. 04
Доступ к информации и ограничения в открытости деятельности государственных органов для общественности
Centre for Integrity in the Defence Sector

GUIDES TO GOOD GOVERN-ANCE
No. 05
Управление рисками коррупции и мошенничества с недвижимостью в оборонном секторе
Centre for Integrity in the Defence Sector

Руководства по надлежащему управлению – это серия небольших по объему брошюр, в каждой из которых обсуждается отдельная тема, важная для надлежащего управления в оборонном секторе. Данные руководства адресованы тем, кто хотел бы расширить знания об одной или нескольких темах, напрямую связанных с надлежащим управлением в оборонном секторе, или, в более широком смысле, в государственном секторе, и могут использоваться в учебных целях.

Полное или частичное воспроизведение руководства разрешено при условии, что будет указано, что материалы полностью принадлежат Центру по укреплению этических основ в оборонном секторе, Осло, Норвегия, и при условии, что любое такое воспроизведение, как в целом, так и частично, не подлежит продаже и не включается в работы, которые продаются.

Издатель: Центр по укреплению этических основ в оборонном секторе
Дизайн: www.melkeveien.no
Опубликовано: Норвежская государственная организация по безопасности и обслуживанию
Май 2018 г. Тираж: 100

Centre for Integrity in the Defence Sector

www.cids.no

NATO OTAN

Перевод оригинальной английской версии на русский язык был любезно предоставлен Организацией Североатлантического договора.