О ратификации Меморандума о понимании между Казахстаном и Организацией НАТО по техническому обслуживанию и обеспечению (НАМСО) по сотрудничеству в области материально-технического обеспечения

Закон Республики Казахстан от 21 июля 2007 года N 295

Ратифицировать Меморандум о понимании между Казахстаном и Организацией НАТО по техническому обслуживанию и обеспечению (НАМСО) по сотрудничеству в области материально-технического обеспечения, подписанный в Брюсселе 1 июля 2003 года.

П р е з и д е н т

Республики Казахстан

Меморандум о понимании между Казахстаном и Организацией НАТО по техническому обслуживанию и обеспечению (НАМСО) по сотрудничеству в области материально-технического обеспечения

Настоящий Меморандум о понимании представляет собой правовую основу для установления отношений между Республикой Казахстан и Организацией НАТО по техническому обслуживанию и обеспечению в области материально-технического обеспечения, изложенных в следующих статьях.

Преамбула

П р и н и м а я в о в н и м а н и е, ч т о:

- Казахстан, приняв приглашение вступить в программу "Партнерство во имя мира" (ПИМ), подписав и присоединившись к Рамочному Документу программы " Партнерство во имя мира" 27 мая 1994 года, является страной-партнером указанной п р о г р а м м ы "П а р т н е р с т в о в о и м я м и р а";

- Министерство обороны Казахстана выразило заинтересованность в услугах, предлагаемых Организацией НАТО по техническому обслуживанию и обеспечению в рамках ее программ и отношений партнерства в области систем вооружения;

- Министерство обороны Казахстана вступает в переговоры с Организацией НАТО по техническому обслуживанию и обеспечению с целью установления сотрудничества в определенных областях материально-технического обеспечения;

- Совет директоров Организации НАТО по техническому обслуживанию и обеспечению согласился предоставлять Казахстану услуги по

материально-техническому обеспечению (как определено далее);

- Совет директоров Организации НАТО по техническому обслуживанию и обеспечению, в контексте сотрудничества с государством-участником программы НАТО "Партнерство во имя мира" (ПИМ), осознает общую заинтересованность стран-членов НАТО в снижении стоимости программ Агентства НАТО по техническому обслуживанию и обеспечению, что является одной из целей, указанных в Уставе Организации НАТО по техническому обслуживанию и обеспечению;

- Североатлантический совет одобрил рекомендации Совета директоров Организации НАТО по техническому обслуживанию и обеспечению о заключении соглашения по техническому обслуживанию и обеспечению с Министерством обороны Казахстана при условии, что вступление в такое соглашение ни при каких обстоятельствах не предоставляет Казахстану статус члена Организации Североатлантического Договора и не дает права Казахстану претендовать на получение такого статуса;

- Совет директоров Организации НАТО по техническому обслуживанию и обеспечению уполномочил Генерального менеджера Агентства НАТО по материально-техническому обеспечению (НАМСА) подписать настоящий Меморандум о понимании.

Казахстан и Организация НАТО по техническому обслуживанию и обеспечению, далее именуемые "Сторонами", достигли понимания по предоставлению материально-технического обеспечения на основе положений, изложенных в настоящем Меморандуме о понимании.

Определения/аббревиатуры

В тексте настоящего Меморандума о понимании и в текстах вытекающих из него конкретных соглашений:

- "НАТО" означает Организацию Североатлантического Договора;

- "НАМСО" означает Организацию НАТО по материально-техническому обслуживанию и обеспечению;

- "НАМСА" означает Агентство НАТО по материально-техническому обслуживанию и обеспечению;

- "ПИМ" означает программу "Партнерство во имя мира", учрежденную на саммите НАТО в Брюсселе 10-11 января 1994 года;

- "Техническая информация" означает записанную или задокументированную информацию научного или технического характера, каковыми бы ни были ее формат, документальные характеристики или способ представления. Эта информация может включать, но не ограничиваться, следующим: экспериментальные данные и данные тестов, технические условия, проекты и процессы проектирования, изобретения и

открытия как патентоспособные, так и непатентоспособные, технические описания и другие работы технического характера, работы по полупроводниковой топографии/ конфигурации масок, пакеты технических и производственных данных, ноу-хау и коммерческие тайны, а также информация, относящаяся к промышленным технологиям. Она может быть представлена в форме документов, графической репродукции, рисунков и других графических представлений, записей на дисках и лентах (оптических, магнитных и лазерных), компьютерного программного обеспечения, относящегося как к программам, так и к базам данных, распечаток компьютерной памяти или данных, хранимых в памяти компьютера, или в любых других формах;

- "ПСВ" означает партнерство в области систем вооружения.

Статья 1
Цель

Настоящий Меморандум о понимании устанавливает официальные рамки для предоставления услуг по материально-техническому обеспечению в явно определенных сферах, включая, но не ограничиваясь, обеспечение, техническое обслуживание, приобретение товаров и услуг, транспортировку, управление конфигурацией и техническую помощь.

Статья 2
Реализация

2.1. Реализация настоящего Меморандума о понимании потребует составления конкретных письменных соглашений, таких как соглашения о продаже, соглашения о предоставлении услуг, соглашения по ПСВ или других.

2.2. При этом понимается, что соглашения, упомянутые в пункте 2.1., и участие в ПСВ могут потребовать предварительного одобрения Министерством обороны Казахстана и потребуют одобрения Советом директоров НАМСО, а также страной происхождения соответствующих систем вооружения или оборудования.

Статья 3
Финансовые договоренности

3.1. Стороны не несут никаких финансовых обязательств в связи с настоящим Меморандумом о понимании, если на иное не дано согласие в силу последующих соглашений таких, как указано в пункте 2.1., и которые относятся к конкретным сферам деятельности и выполняемым задачам.

3.2. При этом понимается, что после подписания соглашения, упомянутого в пункте

2.1., Казахстан, как заказчик, будет нести расходы по оплате услуг, заказанных у НАМСО и предоставленных ею, включая расходы, возникающие в случае прекращения действия Меморандума в соответствии со Статьей 12.

Статья 4
Обязательства, гарантии и страхование

4.1. Каждая из Сторон, получая материалы или услуги по настоящему Меморандуму о понимании, отказывается от претензий по травмам (включая травмы, приведшие к смерти), убыткам или ущербу, если такие травмы, убытки или ущерб возникают в процессе обычного использования и/или эксплуатации таких материалов или услуг.

4.2. Стороны будут оказывать взаимную помощь по защите от претензий или исков какого бы то ни было характера, предъявляемых какой-либо третьей стороной в отношении одной из Сторон с тем, чтобы в конечном итоге защитить поставляющую организацию от такого рода претензий, заявленных третьими сторонами.

4.3. Отказ от претензий и защита от претензий, упомянутых в пунктах 4.1. и 4.2., не применяются к случаям умышленных противоправных действий и грубой небрежности, а также к случаям, конкретно оговоренным в соглашении, заключенном между двумя Сторонами.

4.4. Каждое соглашение вида, указанного в пункте 2.1., будет детализировать гарантию в отношении соответствующих материалов или услуг для каждого рода деятельности и выполняемых задач.

4.5. Отправка грузов, организуемая НАМСО по таким соглашениям, обычно будет происходить без страхования, если на это не поступит конкретный запрос Казахстана. Затраты на такое страхование, которое может быть осуществлено по просьбе Казахстана, будут возмещаться в НАМСО без задержки.

Статья 5
Менеджмент

5.1. Органы, ответственные за управление реализацией настоящего Меморандума о понимании, указаны в Приложении А.

5.2. Для последующих соглашений, указанных в пункте 2.1., Стороны могут назначить конкретные контактные точки.

Статья 6
Требования по безопасности

6.1. Стороны разработают и внедрят скоординированную программу по промышленной безопасности на основе Политики безопасности НАТО (С-М(2002)49 и С-М(2002)50) и Вспомогательных директив к ней.

6.2. Стороны будут уведомлять друг друга о степени секретности, применяемой Стороной-разработчиком к какой-либо информации или данным, передаваемым другой Стороне в соответствии с условиями соглашений, указанных в пункте 2.1.

6.3. Любой обмен секретной информацией, включая контракты, содержащие подобную информацию, должен проводиться в соответствии с условиями Соглашения о безопасности, заключенного 31 июля 1996 года между НАТО и Казахстаном, а также в соответствии с требованиями по безопасности, изложенными в Политике безопасности НАТО (С-М(2002)49 и С-М(2002)50) и Вспомогательных директивах к ней.

Статья 7
Обмен технической информацией, относящейся к правам собственности

7.1. К данным и информации, подлежащим передаче, распространению или обмену другим способом по соглашениям, указанным в пункте 2.1., и которые явным образом определены той или иной Стороной путем нанесения соответствующих штампов, надписей или других письменных обозначений, как относящиеся к правам собственности, применяются следующие условия.

7.2. При этом понимается, что каждая из Сторон берет на себя обязательства:

7.2.1. использовать информацию, принадлежащую другой Стороне, только для целей соглашений, указанных в пункте 2.1.;

7.2.2. обеспечить полную конфиденциальность информации, принадлежащей другой Стороне, и воздерживаться от раскрытия, передачи или другого способа предоставления такой информации третьей стороне;

7.2.3. обращаться с информацией, принадлежащей другой Стороне, как с секретной информацией и обеспечивать ее безопасность, осуществляя те же меры и применяя те же средства контроля в отношении такой информации, какие принимающая Сторона обычно осуществляет и применяет для защиты своей информации, являющейся объектом собственности, в целях недопущения непреднамеренного раскрытия, опубликования, распространения или передачи, а также предпринимать все необходимые действия для обеспечения того, чтобы только сотрудники принимающей Стороны, которым такая информация необходима в силу служебной необходимости, имели доступ к информации, принадлежащей другой Стороне.

7.3. Информация не будет считаться объектом права собственности, и ее использование не будет приводить к возникновению никаких обязательств

принимающей Стороны, если такая информация:

7.3.1. является или становится всеобщим достоянием не по причине злоумышленных или незаконных действий принимающей Стороны;

7.3.2. предоставлена законным образом третьей стороной без подобных ограничений и нарушений настоящего Меморандума о понимании;

7.3.3. одобрена для распространения или использования посредством письменного разрешения передающей Стороны.

7.4. Если между Сторонами не достигнута договоренность об ином, никакие положения соответствующих соглашений вида, упомянутого в пункте 2.1., не будут рассматриваться как предоставляющие какие-либо права или лицензии в отношении любых патентов, изобретений или данных, в любое время находившихся или находящихся в собственности любой из Сторон.

Статья 8
Налоги и пошлины

HAMCO, ее имущество и все виды деятельности освобождаются от:

8.1. всех видов прямых и косвенных налогов; однако HAMCO не будет настаивать на освобождении от налогов и пошлин, которые являются платой за пользование коммунальными услугами;

8.2. таможенных пошлин, ограничений или запретов, связанных с импортом или экспортом товаров личного пользования при условии, что эти импортированные товары не предназначены для продажи в Казахстане;

8.3. таможенных пошлин, ограничений и запретов, связанных с импортом и экспортом печатных материалов.

Статья 9
Процедуры проведения визитов

9.1. Представителям Сторон, по их запросу, будет предоставляться доступ на государственные или частные объекты, на которых проводятся работы, включая тесты и испытания, на основе соглашения, заключенного в рамках настоящего Меморандума о понимании, при условии, что данным представителям это нужно в силу служебной необходимости.

9.2. Организация визитов будет проводиться в соответствии с Инструкциями по безопасности, изложенными в Приложении G к документу C-M(2002)49 под заглавием "Международные визиты". Все посетители будут также соблюдать любые дополнительные требования по обеспечению безопасности и сохранности,

установленные принимающей Стороной. К коммерческим тайнам и другой технической информации, сообщаемой посетителям, применяются те же правила, как если бы они были переданы Стороне, направляющей посетителей.

Статья 10
Язык

Будет применяться обычная политика НАТО, предусматривающая ведение всей официальной документации на английском и французском языках.

Статья 11
Поправки

Положения настоящего Меморандума о понимании могут быть изменены посредством письменного соглашения Сторон.

Статья 12
Прекращение действия

12.1. Если одна из Сторон намерена выйти из настоящего Меморандума о понимании или одного из последующих соглашений, упомянутых в пункте 2.1., то эта Сторона предоставит другой Стороне письменное уведомление за шесть месяцев до 1 января данного года.

12.2. В случае выхода из Меморандума о понимании или из одного из последующих соглашений, упомянутых в пункте 2.1., Стороны своевременно проконсультируются друг с другом относительно наиболее удовлетворительных условий выхода.

12.3. В случае, если того требует уведомление о выходе, Стороны начнут переговоры по каждому соглашению вида, указанного в пункте 2.1., о возможно более ранней дате выхода и решении финансовых вопросов в отношении выполняемых задач и оказываемых услуг, на которых отразится выход. Сторона, заявившая о выходе, полностью выполнит свои обязательства к дате прекращения действия Меморандума.

12.4. Если Стороны совместно решат прекратить действие настоящего Меморандума о понимании, то они совместно будут нести расходы по прекращению его действия.

12.5. Права и обязанности Сторон в отношении раскрытия и использования технической информации, безопасности, продажи и передачи третьим сторонам, решения споров, претензий и обязательств, а также выхода и прекращения действия Меморандума будут сохраняться независимо от выхода одной из Сторон из настоящего Меморандума о понимании или прекращения его действия или вытекающих из него соглашений вида, указанного в пункте 2.1.

Статья 13
Решение споров

Любые разногласия, возникающие между Сторонами, связанные с толкованием или применением настоящего Меморандума о понимании, будут решаться в ходе переговоров между ними без привлечения внешней юрисдикции или третьей стороны.

Статья 14
Вступление в силу

Настоящий Меморандум о понимании вступает в силу в день его подписания последней из Сторон.

Статья 15
Подписание

Вышеприведенные статьи отражают взаимопонимание, достигнутое между Казахстаном и НАМСО. Два подлинных экземпляра исполнены на английском и французском языках каждый, и надлежащим образом подписаны. Тексты на обоих языках имеют одинаковую силу.

От имени Правительства Республики Казахстан

Тулеутай Сулейменов

Чрезвычайный и Полномочный Посол

_____

Дата: 1 июля 2003 года

От имени Организации НАТО по техническому обслуживанию и обеспечению

Питер Марки

Генеральный менеджер

_____

Дата: 1 июля 2003 года

Приложение А

Органами контактирования по всем вопросам относительно положений настоящего Меморандума являются:

От Министерства обороны Казахстана:
Представительство Казахстана в НАТО
B-1110, г. Брюссель
тел.: 0032 2 374 9562
факс: 0032 2 374 5091

От Организации НАТО по техническому обслуживанию и обеспечению (НАМСО):
Советник по юридическим вопросам
L-8302, Капеллен

г. Люксембург
тел.: 00352-3063 6554

факс: 00352-308721

Настоящим удостоверяю, что данный текст является неофициальным переводом на русский язык Меморандума о понимании между Казахстаном и Организацией НАТО по техническому обслуживанию и обеспечению (НАМСО) по сотрудничеству в области материально-технического обеспечения, подписанного в городе Брюссель 31 июля 1996 года.

Начальник Главного управления
международных программ
Вооруженных Сил Республики Казахстан
полковник *В. Райхель*

НАТО НЕСЕКРЕТНО

СЕВЕРОАТЛАНТИЧЕСКИЙ СОВЕТ

17 июня 2002 года **ДОКУМЕНТ С-М(2002)49**

БЕЗОПАСНОСТЬ В РАМКАХ ОРГАНИЗАЦИИ СЕВЕРОАТЛАНТИЧЕСКОГО ДОГОВОРА (НАТО)

Примечание Генерального секретаря

Ссылка: *С-М* (2002) 23 и Перечень его мероприятий

1. Настоящий документ является результатом Фундаментального обзора, проведенного Комитетом безопасности НАТО, и был одобрен Советом по процедуре умолчания 26 марта 2002 года.

2. Настоящий документ, наряду с документом *С-М* (2002)49 "Меры защиты гражданских и военных органов НАТО, развернутых сил и объектов (средств) НАТО против угрозы терроризма" отменяет действие документа *С-М* (55)15 *(Final).* За исключением Приложения А "Соглашение между участниками Североатлантического договора о безопасности", которое по-прежнему является действующим для стран, не ратифицировавших "Соглашение между участниками Североатлантического договора о безопасности информации", все предшествующие версии документа *С-М* (55)15 *(Final)* должны быть уничтожены.

Настоящий документ поддерживают следующие директивы:

AC/35-D/2000 Директива о безопасности персонала

AC/35-D/2001 Директива о физической безопасности

AC/35-D/2002 Директива о безопасности информации

AC/35-D/2003 Директива о промышленной безопасности

AC/35-D/2004 Основная директива о безопасности информации

AC/35-D/2005 Директива об управлении информационной безопасностью для *CIS*

Первые четыре директивы (*AC*/35-*D*/2000-2003) утверждены Советом, последние две *AC/*35-D/2004 и *AC*/35-D/2005 утверждены Комитетом безопасности НАТО и Советом командования, управления и связи НАТО.

3. Для удобства при упоминании, перечень/компендиум, содержащий оба документа по политике в области безопасности (*C-M* (2002)49 и *C-M* (2002)50), а также указанные выше директивы в поддержку, будут разосланы в ближайшем будущем всем текущим держателям *C-M* {55)15 *{Final)* .

(Подписано) Джордж Робертсон

Оригинал: английский

ЛИСТ ЗАПИСИ ПОПРАВОК

Зачеркните соответствующий номер каждой из вложенных поправок

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

СОДЕРЖАНИЕ

Приложение "А" к C-M(2002)49

ПРИЛОЖЕНИЕ "А"
СОГЛАШЕНИЕ МЕЖДУ УЧАСТНИКАМИ СЕВЕРОАТЛАНТИЧЕСКОГО ДОГОВОРА О БЕЗОПАСНОСТИ ИНФОРМАЦИИ[1]

Участники Североатлантического договора, подписанного в Вашингтоне 4 апреля 1 9 4 9 г о д а ;

Подтверждая, что эффективные политические консультации, сотрудничество и оборонное планирование при реализации целей Договора предполагают обмен секретной информацией между участниками;

Учитывая необходимость соглашений между правительствами участников Североатлантического договора о взаимной защите и охране обмениваемой секретной и н ф о р м а ц и и ;

Осознавая потребность в установлении общих рамок в отношении стандартов и п р о ц е д у р б е з о п а с н о с т и ;

Представляя национальные интересы и интересы Организации североатлантического договора, достигли договоренности о нижеследующем:

СТАТЬЯ 1

(i) з а щ и щ а т ь и о х р а н я т ь :

(a) секретную информацию (см. ПРИЛОЖЕНИЕ 1), отмеченную как таковую, исходящую из НАТО (см. ПРИЛОЖЕНИЕ 2) или переданную в НАТО г о с у д а р с т в о м - ч л е н о м ;

(b) секретную информацию, отмеченную как таковую, переданную одним государством-членом другому государству-члену в поддержку программ, проектов и к о н т р а к т о в Н А Т О ;

(ii) поддерживать категорию/гриф секретности информации в соответствии с пунктом (i) настоящей статьи и прилагать все усилия для обеспечения ее с о о т в е т с т в у ю щ е й з а щ и т ы ;

(iii) использовать секретную информацию, определенную в пункте (i) настоящей статьи, исключительно в целях, изложенных в Североатлантическом договоре, а также в соответствии с относящимися к нему решениями и резолюциями;

(iv) не раскрывать секретную информацию, определенную в пункте (i) настоящей статьи, государствам, не являющимся членами НАТО, без согласия источника.

СТАТЬЯ 2

Согласно Статье 1 настоящего Соглашения, участники должны учредить Национальный орган безопасности, ответственный за соблюдение мер безопасности при проведении мероприятий НАТО. Участники должны разработать и применить стандарты безопасности, обеспечивающие общий уровень защиты секретной информации.

---

[1] Данное соглашение в настоящий момент находится на этапе ратификации

правительствами следующих государств-членов НАТО: Бельгия, Исландия, Италия, Люксембург, Норвегия, Португалия, Испания, и Объединенное Королевство. " Соглашение между участниками Организации североатлантического договора о безопасности", содержащееся в приложении А к документу *C-M* (55)15 *(Fina[)* остается в силе применительно государствам, не ратифицировавшим настоящее соглашение.

СТАТЬЯ 3

(1) Участники должны провести соответствующую проверку всех представляющих их лиц, выполнение функциональных обязанностей которых требует или может требовать предоставления доступа к информации, имеющей гриф "Конфиденциально" и выше, перед их вступлением в должность.

(2) Процедура оформления допуска должна быть нацелена на определение возможности предоставления доступа к секретной информации лицу, исходя из его преданности и благонадежности, не подвергая безопасность неприемлемому риску.

(3) По требованию, каждый из участников должен оказать содействие другим участникам при проведении ими соответствующих процедур по оформлению допуска.

СТАТЬЯ 4

Генеральный секретарь несет ответственность за соблюдение соответствующих условий настоящего Соглашения в рамках НАТО (см. ПРИЛОЖЕНИЕ 3).

СТАТЬЯ 5

Настоящее Соглашение никоим образом не препятствует заключению Сторонами других Соглашений в отношении обмена секретной информацией, инициированных ими и не влияющих на предмет настоящего Соглашения.

СТАТЬЯ 6

(a) Настоящее Соглашение подписывается участниками Североатлантического договора и подлежит ратификации, принятию и утверждению. Документы ратификации, принятия и утверждения должны быть переданы на хранение Правительству Соединенных Штатов Америки.

(b) Настоящее Соглашение вступает в силу через 30 (тридцать) дней после предоставления двумя подписавшими государствами своих документов ратификации, принятия и утверждения. Для каждого другого подписавшего государства настоящее Соглашение вступает в силу через 30 (тридцать) дней после предоставления собственных документов ратификации, принятия и утверждения.

(c) Настоящее Соглашение для сторон, в отношении которых оно вступило в силу,

заменяет собой "Договор о безопасности Сторон по отношению к Организации Североатлантического договора" утвержденный Североатлантическим советом в Приложении А (параграф 1) к дополнению Приложения *D.C. 2/7* от 19 апреля 1952 года , и впоследствии изложенный в Приложении "А" (параграф 1) к *C-M* (55)15 (окончательный), утвержденный Североатлантическим советом 2 марта 1955 года.

СТАТЬЯ 7

Настоящее Соглашение будет открытым для присоединения любой новой Стороны к Североатлантическому договору в соответствии с конституционными процедурами Сторон. Документы Сторон о присоединении к международному договору должны быть переданы на хранение Правительству Соединенных Штатов Америки. Для каждого другого присоединившегося Государства, настоящее Соглашение вступает в силу через 30 (тридцать) дней после предоставления собственных документов Государства о присоединении к международному договору.

СТАТЬЯ 8

Правительство Соединенных Штатов Америки должно информировать Правительства других Сторон о хранении документов ратификации, принятия и утверждения или присоединения.

СТАТЬЯ 9

Настоящее Соглашение может быть прекращено любой Стороной письменным уведомлением депозитария о денонсировании, который должен проинформировать все другие Стороны о получении такого уведомления. Такая денонсация вступает в силу по истечению одного года с получения депозитарием уведомления, но не должна повлиять на уже обусловленные договором обязательства и права или прерогативы, ранее принятые Сторонами, в соответствии с условиями настоящего Соглашения.

В подтверждении чего нижеподписавшиеся, наделенные с этой целью надлежащими полномочиями соответствующих Правительств, подписали настоящее Соглашение.

Совершено в Брюсселе, ____ числа _____ года в единственном экземпляре на английском и французском языках, каждый текст имеет одинаковую силу и должен быть помещен в архив депозитария Правительства США, и заверенные копии должны быть переданы Правительствам, подписавшим документ.

НАТО НЕСЕКРЕТНО

П р и л о ж е н и е " А " к C-M(2002)49

ПРИЛОЖЕНИЕ 1

Это приложение является неотъемлемой частью Соглашения.

Определение секретной информации НАТО включает в себя:

(a) информация - сведения, которые можно передавать в любой форме;

(b) секретной информацией является информация или материал, требующие защиты от несанкционированного разглашения, и которые были охарактеризованы таковыми по классификации безопасности;

(c) понятие "материалы" включает в себя документы, а также любые элементы механизмов, оборудования/компонентов или вооружения либо произведенных, либо находящихся в процессе производства;

(d) понятие "документ" означает любую записанную информацию независимо от ее физической формы или характеристик, включая, без ограничений, письменную и печатную продукцию, карточки и записи обработанных данных, карты, чертежи, фотографии, изображения, рисунки, гравюры, наброски, рабочие записи и бумаги, машинописные копии или копировальные ленты, или репродукция, выполненная любым способом или процессом, а также звуковые, голосовые, магнитные, электронные, оптические или видео записи в любой форме, и портативное оборудование для автоматической обработки данных со стационарных или съемных компьютерных носителей данных.

ПРИЛОЖЕНИЕ 2

Это Приложение является неотъемлемой частью Соглашения.

В целях настоящего Соглашения, термин "НАТО" означает Организацию североатлантического договора и органы, управляемые либо Соглашением по статусу Организации североатлантического договора, национальных представителей и международного штаба, подписанного 20 сентября 1951 года в Оттаве или Протоколом по статусу Международных военных штабов, созданных в соответствии с Североатлантическим Договором, подписанным в Париже 28 августа 1952 года.

ПРИЛОЖЕНИЕ 3

Это Приложение является неотъемлемой частью Соглашения.

Консультация проходит с участием военачальников с целью уважения их прерогативы (исключительного права).

Приложение "B" к C-M(2002)49

ПРИЛОЖЕНИЕ "B"
ОСНОВНЫЕ ПРИНЦИПЫ И
МИНИМАЛЬНЫЕ СТАНДАРТЫ БЕЗОПАСНОСТИ

ВВЕДЕНИЕ

1. Настоящий *C-M* устанавливает основные принципы и минимальные стандарты безопасности, применяемые странами, входящими в НАТО и гражданскими и военными организациями НАТО с целью гарантирования общего уровня защиты обмена классифицированной информацией между сторонами. Процедуры безопасности НАТО действуют с наибольшей пользой, только когда они основываются и поддерживаются системами национальной безопасности, имеющими характеристики, изложенные в настоящем Приложении. Настоящее Приложение также представляет ответственность по безопасности в НАТО.

ЦЕЛИ И ЗАДАЧИ

2. Страны, входящие в НАТО, гражданские и военные организации НАТО должны гарантировать применение основных принципов и минимальных стандартов безопасности, изложенных в настоящем *C-M* для защиты конфиденциальности классифицированной информации, ее целостности.

3. Страны, входящие в НАТО, гражданские и военные организации НАТО должны установить программы безопасности, отвечающие основным принципам и минимальным стандартам безопасности, гарантирующие общий уровень защиты классифицированной информации.

ПРИМЕНЕНИЕ

4. Настоящие основные принципы и минимальные стандарты безопасности должны быть применены к:

(a) классифицированной информации, создаваемой НАТО, созданной страной-членом НАТО и представленной в НАТО или представленной страной-членом НАТО другой стране-члену НАТО в поддержку программ, проектов или контрактов НАТО;

(b) классифицированной информации, полученной НАТО от источников стран, не являющихся членами НАТО; и

(c) классифицированной информации, вверенной отдельным личностям или организациям, не входящим в правительство (или гражданские и военные организации НАТО), например, консультанты (советники), промышленность, университеты, которые должны защищать ее в соответствии с теми же стандартами, которые применяются правительством или гражданскими или военными организациями НАТО.

5. Доступ и защита информации о ядерном оружии *(ATOMAL)* является предметом Соглашения между Сторонами Североатлантического договора по сотрудничеству в отношении информации о ядерном оружии - *C-M* (64)39. Административные меры для

исполнения Соглашения между Сторонами Североатлантического договора по сотрудничеству в отношении информации о ядерном оружии (*АТОМАЛ)* - текущая версия *С- М* (68)41 о будут использованы для контроля доступа, обращения и защиты такой информации.

6. Доступ и защита информации о Едином комплексном оперативном плане США *(US-SIOP)*, является предметом положений *С-М* (71)27 (Измененный), "Специальные процедуры по обращению с информацией по единому комплексному оперативному плану США в рамках НАТО".

7. Секретный характер криптографической информации, мер и продуктов, требует применения строгих мер безопасности, часто помимо тех, что изложены в настоящем *С-М*. Поэтому, доступ и защита криптографической информации, мер и продуктов утвержденных страной или Военным комитетом НАТО, должны быть в согласовании с Приложением "Е", поддерживающими директивами и процедурами, установленными соответствующими властями.

ВЛАСТЬ

8. Североатлантический совет *(NAC)* утвердил этот документ, обеспечивающий выполнение Соглашения между Сторонами к Североатлантическому договору по безопасности информации (воспроизведенный в Приложении "А"), и таким образом определяющий Политику безопасности НАТО.

ОСНОВНЫЕ ПРИНЦИПЫ

9. Следующие основные принципы должны быть применены:

(a) страны НАТО и гражданские и военные организации НАТО должны гарантировать, что минимальные стандарты, изложенные в настоящем *С-М*, приняты для гарантирования общей степени защиты классифицированной информации, которой стороны обмениваются между собой;

(b) классифицированная информация должна распространяться исключительно на основе принципа служебной необходимости персоналу, который был проинформирован по соответствующим процедурам безопасности; в дополнение, только лица, проверенные на благонадежность, имеют допуск к классифицированной информации с грифом КОНФИДЕНЦИАЛЬНО и выше;

(c) руководство по принятию мер по снижению риска с точки зрения обеспечения безопасности классифицированной информации, должно быть обязательным в военных и гражданских органах НАТО. Принятие таких мер в пределах стран-членов НАТО необязательно;

(d) классифицированная информация должна охраняться сбалансированным комплексом мер по безопасности, включая кадровые, физические, меры безопасности

информации и информационных систем *(INFOSEC)*, которые должны распространяться на всех лиц, имеющих доступ к классифицированной информации, всей информации проходящей по СМИ, и всех предпосылок, содержащих такую информацию;

(e) все подозрительные факты нарушения безопасности должны незамедлительно докладываться соответствующему руководству, отвечающему за безопасность. Доклады должны быть оценены соответствующими официальными лицами на предмет нанесения ущерба НАТО и принятию соответствующих мер действия. Приложение "Е" предоставляет детальную информацию в этом отношении;

(f) составители секретных документов распространяют их в НАТО и для стран НАТО в рамках программ, проектов или контрактов НАТО с пониманием того, что с ними будут обращаться и они будут защищаться в соответствии со стратегией НАТО по управлению информацией и политикой НАТО в области безопасности;

(g) классифицированная информация является предметом контроля со стороны составителя;

(h) распространение классифицированной информации должно осуществляться в соответствии с требованиями Приложения "Е" к настоящему *C-M* и соответствующих инструкций;

(i) являясь предметом согласия со стороны составителя и в соответствии с Приложением "Е" настоящего *C-M*, классифицированная информация НАТО должна передаваться только тем странам и организациям не являющимся членами НАТО, которые имеют подписанное Соглашение по безопасности с НАТО или предоставивших НАТО гарантии по безопасности, либо прямо либо посредством стран НАТО или военных и гражданских органов НАТО, организующих распространение. Во всех случаях распространения классифицированной информации НАТО, должны быть соблюдены те степени защиты, которые оговорены настоящим *C-M*.

10. Принципы, имеющие отношение к национальной безопасности:

(a) организация по безопасности отвечает за:

(i) сбор и запись разведывательной информации касательно шпионажа, терроризма, террористов, диверсии, угроз подрывной деятельности; и

(ii) сосредоточение такой информации, с тем, чтобы она могла быть использована в любой ситуации имеющей отношение к приему персонала на работу правительственными ведомствами и государственными учреждениями и подрядчиками; и

(iii) предоставление информации и рекомендаций Правительству по характеру угроз безопасности и средств защиты против них; и

(b) постоянное сотрудничество между правительственными ведомствами и государственными учреждениями:

(i) определение классифицированной информации, которую необходимо

защитить; и

(ii) устанавливать и применять общие степени защиты, как изложено в настоящем *С-М.*

ДОСТУП ПЕРСОНАЛА К КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИИ

11. Процедуры личной безопасности должны быть разработаны с оценкой возможности персонала иметь первоначальный или постоянный доступ к классифицированной информации без нанесения риска безопасности, принимая во внимание его преданность, кредитоспособность и надежность. Все гражданские и военные, которым необходим доступ или чьи функциональные и служебные обязанности могут позволить доступ к классифицированной информации с грифом КОНФИДЕНЦИАЛЬНО или выше, должны быть соответствующим образом проверены и проинструктированы перед получением доступа. Лицо должно получать доступ к классифицированной информации НАТО только по мере служебной необходимости.

12. Проверка на благонадежность не требуется для допуска к информации с грифом ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ; такие лица должны быть проинформированы об их ответственности за защиту информации ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ.

13. Безопасность персонала представлена далее в Приложении "С" настоящего *С-М* и в соответствующих инструкциях по безопасности персонала.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

14. Физическая безопасность это применение физических мер по защите мест, зданий или помещений содержащих информацию, требующую защиты против утери или компрометации. Программы физической защиты, состоящие из активных и пассивных мер безопасности, должны быть установлены для обеспечения уровней физической безопасности согласующейся с угрозой, грифом секретности и количеством информации требующей защиты.

15. Физическая безопасность представлена далее в Приложении "D" настоящего *С-М* и в инструкции по обеспечению физической безопасности.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

16. Безопасностью информации является применение общих мер по защите и процедур по предотвращению, обнаружению или вскрытию утери информации или ее рассекречивания. Классифицированная информация должна быть защищена на протяжении всего жизненного цикла на уровне, соизмеримом с уровнем секретности.

Должны быть достигнуты гарантии применения соответствующего грифа секретности, четкого определения информации как секретной, и информация должна оставаться классифицированной только необходимое время.

17. Гриф секретности, применяемый к информации, должен указывать на возможный урон безопасности НАТО и/или стран-членов НАТО, в случае если эта информация будет являться предметом несанкционированного раскрытия.

Гриф секретности НАТО должен быть наложен в соответствии с Приложением "Е" настоящего *С-М*. Определение и изменение грифа секретности является прерогативой составителя информации.

18. Грифы секретности НАТО и их определения:

(a) СОВЕРШЕННО СЕКРЕТНО *(CTS)* - несанкционированное раскрытие может привести к очень серьезному урону безопасности НАТО;

(b) НАТО СЕКРЕТНО *(NS)* - несанкционированное раскрытие может привести к серьезному урону безопасности НАТО;

(c) НАТО КОНФИДЕНЦИАЛЬНО *(NC)* - несанкционированное раскрытие может привести к урону безопасности НАТО;

(d) НАТО ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ *(NR)* - несанкционированное раскрытие может причинить ущерб интересам и эффективности НАТО.

19. Засекречивая информацию, составитель должен принять во внимание урон, который настоящая информация может нанести в случае несанкционированного раскрытия, и должен указать, где это возможно, известную дату или событие, когда может быть снижена категория секретности информации или ее рассекречивание.

20. Информация грифа НАТО НЕСЕКРЕТНО - политика и процедуры для управления и защиты неклассифицированной информации с грифом НАТО НЕСЕКРЕТНО представлена в Процедурах НАТО по Управлению Информационными потоками *(NIMP)*.

21. Безопасность информации представлена далее в Приложении "Е" настоящего *С-М* и в информационных инструкциях по обеспечению безопасности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (INFOSEC)

22. *INFOSEC* это применение мер безопасности по защите информации имеющейся, хранящейся или передаваемой по средствам связи, системы информационного обслуживания и другие электронные системы, против утраты конфиденциальности, целостности или доступности, как случайной, так и преднамеренной, и для предотвращения утраты целостности или доступности самих систем. Для достижения задач безопасности по секретности, целостности и доступности хранения классифицированной информации, обработке или передачи средствами связи, информационных и других электронных систем, должны быть применены

сбалансированные комплексы мер по безопасности (физические, кадровые, безопасности информации и *INFOSEC*) для создания безопасной среды, в которой действуют системы связи, информации и другие электронные системы.

23. *INFOSEC* представлена далее в Приложении "F" настоящего *C-M*, в директивах по обеспечению руководства *INFOSEC*, Технических директивах *INFOSEC* и директивах *INFOSEC* по Применению.

ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ

24. Промышленной бесопасностью является применение защитных мер и процедур по предупреждению, обнаружению и восстановлению от потери или несанкционированного разглашения классифицированной информации, обращаемой в промышленности при выполнении контрактов. Классифицированная информация НАТО доводится промышленности в результате контракта, и секретные контракты с промышленностью должны быть защищены в соответствии с Политикой безопасности НАТО и соответствующими инструкциями.

25. Перед тем как предприятия и их персонал, руководящий состав или владельцы могут получить доступ к классифицированной информации, или быть приглашенными для участия в конкурсе, в переговорном процессе, или выполнять секретный контракт, или работать в области секретных исследований, включающих в себя доступ к классифицированной информации с грифом КОНФИДЕНЦИАЛЬНО или выше, предприятие должно получить допуск к работе с классифицированной информацией, выданный национальным органом безопасности *(NSA)* (или, при необходимости, назначенными органами национальной безопасности) страны происхождения, другими словами, страной, в которой предприятие расположено и зарегистрировано для ведения бизнеса.

26. Предприятия должны защищать классифицированную информацию в соответствии с основными принципами и минимальными стандартами, содержащимися в настоящем *C-M*. Национальные органы безопасности *(NSA)* должны гарантировать наличие у них средств, обязывающих промышленность выполнять требования по промышленной безопасности и наличие прав по инспектированию и санкционированию мер, принятых промышленностью по защите классифицированной информации.

27. Промышленная безопасность представлена далее в Приложении "G" настоящего *C-M* и в соответствующих инструкциях по промышленной безопасности.

ЗАЩИТА ИНФОРМАЦИИ ПО КЛЮЧЕВЫМ ПУНКТАМ

28. Публикация информации о гражданских объектах (поставляющих оборонную продукцию, обеспечивающих энергией и так далее) имеющих военную значимость во

время напряженной ситуации или в военное время, может содействовать проведению бомбардировки, саботажа или террористической атаки путем позволения потенциальному противнику собирать сведения о списке объектов, имеющих ключевое значение и определять объекты уязвимые к проведению саботажа или терроризма. Должна быть разработана стратегия поведения, препятствующая составлению потенциальным противником Списка ключевых объектов, разрешающая в целях обеспечения безопасности, применять изъятия из публикаций соответствующей информации и способствующая осведомленности о рисках среди владельцев и управляющих объектами.

ОТВЕТСТВЕННОСТЬ ПО БЕЗОПАСНОСТИ

Полномочия национальных органов безопасности (NSA)

29. Каждая страна должна создать национальные органы безопасности *(NSA)*, ответственные за безопасность классифицированной информации НАТО.

30. Национальные органы безопасности *(NSA)* ответственны за:

(a) поддержание безопасности классифицированной информации НАТО в государственных учреждениях и их компонентах, военных и гражданских, в стране и за границей;

(b) гарантирование периодического проведения соответствующих проверок по мерам защиты классифицированной информации НАТО во всех государственных организациях на всех уровнях, как военных, так и гражданских, для определения адекватности принятых мер в соответствии с текущими правилами безопасности НАТО. В случае, если организация обладает информацией с грифом СОВЕРШЕННО СЕКРЕТНО *(CTS)* или в отношении ядерного оружия *(ATOMAL)*, проверки безопасности должны осуществляться, по крайней мере, один раз в 18 месяцев, за исключением, если за этот период они были проведены Офисом безопасности НАТО *(NOS)*.

(c) гарантирование того, что решение на проверку по безопасности было сделано с уважением всех граждан, которым необходим допуск к классифицированной информации с грифом *(NC)* и выше в соответствии с Политикой безопасности НАТО;

(d) гарантирование наличия государственных планов по безопасности в случае чрезвычайных ситуаций в целях предотвращения попадания классифицированной информации НАТО лицам, не имеющим на это санкции или в руки противника; и

(e) санкционирование составления (или аннулирование) государственного основного Регистра совершенно секретной информации. Офис безопасности НАТО *(NOS)* должен быть уведомлен о составлении (или аннулировании) государственного основного Регистра совершенно секретной информации.

Назначенные органы безопасности (DSA)

31. Каждая страна-член НАТО может определить один или более назначенный орган безопасности *(DSA)*, ответственный за национальные органы безопасности *(NSA)*. В этом случае, назначенный орган безопасности *(DSA)* страны-члена НАТО отвечает за связь промышленности с государственной политикой и всеми вопросами политики промышленной безопасности НАТО и за предоставление инструкций и содействия в их осуществлении. В некоторых государствах, функции (DSA) могут выполняться национальным органом безопасности (NSA).

Комитет по вопросам безопасности НАТО (NSC)

32. Комитет по вопросам безопасности НАТО *(NSC)* учреждается Североатлантическим Советом *(NAC)* и состоит из представителей стран-членов НАТО имеющих опыт работы в сфере вопросов безопасности в своих странах.

Комитет по вопросам безопасности НАТО *(NSC)* напрямую подчиняется Североатлантическому Совету *(NAC)*. Представители Военного комитета НАТО *(NAMILCOM)* должны присутствовать на встречах Комитета по вопросам безопасности НАТО *(NSC)*. Представители военных и гражданских органов НАТО также могут присутствовать, в случае если имеют отношение к вопросам обсуждения.

33. Комитет по вопросам безопасности НАТО *(NSC)* напрямую отвечает перед Североатлантическим Советом *(NAC)* за:

(a) экспертизу вопросов в отношении Политики безопасности НАТО;

(b) рассмотрение вопросов безопасности переданных Североатлантическим Советом *(NAC)*, страной-членом НАТО. Генеральным Секретарем, Военным комитетом НАТО *(NAMILCOM)*, или Главами военных и гражданских органов НАТО; и

(c) подготовку соответствующих рекомендаций Североатлантическому Совету *(NAC)*.

Офис безопасности НАТО (NOS)

34. Офис безопасности НАТО *(NOS)* учрежден в рамках международного штаба НАТО. Офис состоит из персонала, имеющего опыт работы в области безопасности, как в военной, так и в гражданской сферах. Офис поддерживает тесные связи с национальными органами безопасности *(NSA)* каждой страны-члена НАТО, и с военными и гражданскими органами НАТО. Также, если потребуется, Офис может просить страны-члены НАТО, военные и гражданские органы НАТО о выделении дополнительного персонала для оказания содействия в течение короткого промежутка

времени в случае, когда привлечение дополнительного персонала на полный рабочий день в Офисе будет не оправданным. Директор Офиса безопасности НАТО *(NOS)* является Председателем Комитета по вопросам безопасности НАТО *(NSC)*.

35. Офис безопасности НАТО *(NOS)* отвечает за:

(a) экспертизу любых вопросов влияющих на безопасность НАТО;

(b) определение средств, на основании которых безопасность НАТО может быть улучшена;

(c) общую координацию вопросов безопасности для НАТО среди стран-членов и военных и гражданских органов НАТО;

(d) гарантирование исполнения решений НАТО по безопасности, включая предоставление таких советов которые могут быть запрошены страной-членом НАТО и военными и гражданскими органами НАТО, либо по применению ими основных принципов и стандартов безопасности, описанных в настоящем приложении, или в исполнении специальных требований по безопасности.

(e) информирование соответствующим образом Комитета по вопросам безопасности НАТО *(NSC)*, Генерального Секретаря и Председателя военного Комитета в заданном порядке в пределах НАТО и сделанном прогрессе в исполнении решений Североатлантического Совета *(NAC)* в отношении вопросов безопасности;

(f) выполнение периодических инспекционных проверок систем безопасности по защите классифицированной информации НАТО в странах-членах НАТО, военных и гражданских органах НАТО, Штабе верховного главнокомандующего объединенными вооруженными силами НАТО в Европе *(SHAPE)*, и верховного главнокомандования объединенными вооруженными силами НАТО на Атлантике *(SACLANT)*;

(g) координацию с национальным органом безопасности *(NSA)* и военными и гражданскими органами НАТО, проведения расследований в случае утери, разглашения или возможного разглашения классифицированной информации НАТО;

(h) информирование национальных органов безопасности *(NSA)* о любой информации враждебной интересам НАТО, которая приводит к восприятию озабоченности их стран;

(i) разработку мер безопасности по защите Штабов НАТО в Брюсселе и гарантию их правильного исполнения; и

(j) выполнение под руководством и по поручению Генерального Секретаря, от имени Североатлантического Совета (NAC) и под их руководством, обязанностей по контролю применения программ безопасности НАТО по защите информации о ядерном оружии (ATOMAL) в рамках Соглашений и обеспечивающих Административных Соглашений, приведенных выше в параграфе 5.

Военный комитет НАТО и Военные органы НАТО

36. Как высшее военное руководство в НАТО, (NAMILCOM) ответственен за общее управление военными вопросами. Таким образом, Военный комитет НАТО несет ответственность за все вопросы безопасности в военных структурах НАТО, включая централизованную и общую юрисдикцию мер, необходимых для гарантирования адекватности шифровальной техники и материалов, используемых при передаче классифицированной информации НАТО, включая санкционирование с точки зрения безопасности работы средств шифровальной аппаратуры, как определено в Приложении "F".

В соответствии с ранее согласованной политикой и в соответствии с положениями параграфа 35 выше, (NOS) выполняют функции по безопасности в пределах военных структур НАТО и информируют Председателя Военного комитета НАТО.

37. Главы военных органов НАТО, учрежденные под эгидой Военного комитета НАТО (NAMILCOM), ответственны за вопросы безопасности в пределах своих учреждений. Это включает ответственность за гарантирование того, что организационные структуры безопасности установлены, программы безопасности разработаны и исполнены в соответствии с Политикой безопасности НАТО, и, что меры по безопасности периодически инспектируются на каждом командном уровне. В случаях, если организации располагают информацией с грифом СОВЕРШЕННО СЕКРЕТНО (CTS) или имеющей отношение к ядерному оружию (ATOMAL), проверки по безопасности должны осуществляться по крайней мере, один раз каждые 18 месяцев , за исключением, если за этот период они были проведены Офисом безопасности НАТО (NOS).

Гражданские органы НАТО

38. Международный штаб НАТО и гражданские учреждения НАТО несут ответственность перед Североатлантическим Советом (NAC) за соблюдение безопасности в пределах своих заведений. Это включает ответственность за гарантирование того, что организационные структуры безопасности установлены, программы безопасности разработаны и исполнены в соответствии с Политикой безопасности НАТО и, что меры по безопасности периодически инспектируются на каждом командном уровне. В случаях, если организации располагают информацией с грифом СОВЕРШЕННО СЕКРЕТНО (CTS) или имеющей отношение к ядерному оружию (ATOMAL), проверки по безопасности должны осуществляться по крайней мере, один раз каждые 18 месяцев, за исключением, если за этот период они были проведены Офисом безопасности НАТО (NOS).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (INFOSEC)

39. Основные организации, отвечающие за информационную безопасность (например, Совет НАТО по консультациям, командованию и управлению (NC3B), Национальные органы безопасности связи (NCSA) и Национальные органы распространения (NDA)) описаны в Приложении "F".

КООРДИНАЦИЯ БЕЗОПАСНОСТИ

40. Любые проблемы безопасности, требующие координации между национальными органами безопасности (NSA) стран-членов НАТО и военными и гражданскими органами НАТО, должны быть переданы на рассмотрение в Офис безопасности НАТО (NOS). В случаях, когда такая передача осуществляется военным руководством, это должно пройти по командной инстанции. Любые неразрешенные разногласия возникающие в течение такого сотрудничества, должны быть представлены Офисом безопасности НАТО (NOS) на рассмотрение Комитета по вопросам безопасности НАТО (NSC).

41. Любые предложения стран-членов НАТО и военных и гражданских органов НАТО, вносящие изменения в процедуры безопасности НАТО, должны быть рассмотрены в первой инстанции в Офисе безопасности НАТО (NOS). Любые предложения военного руководства должны пройти по командной инстанции. Если проблемы безопасности НАТО, возникшие в НАТО, могут быть решены только путем изменения Политики безопасности НАТО, предложения должны быть направлены на рассмотрение в Комитет по вопросам безопасности НАТО (NSC) и, если необходимо, Комитетом по вопросам безопасности НАТО (NSC) в Североатлантический Совет (NAC).

ПРИЛОЖЕНИЕ "C"
БЕЗОПАСНОСТЬ ПЕРСОНАЛА

ВВЕДЕНИЕ

1. Настоящее Приложение четко излагает политику и минимальные стандарты безопасности персонала. Подробные данные находятся в соответствующей инструкции по безопасности персонала.

2. Должны быть установлены оговоренные стандарты уверенности в лояльности, надежности и достоверности в отношении индивидов, имеющих доступ или обязанности и функции, которые позволяют иметь доступ к секретной информации НАТО. Все лица, гражданские или военные, обязанности которых требуют наличие доступа к информации под грифом НАТО КОНФИДЕНЦИАЛЬНО или выше, должны достаточным образом проверяться для получения удовлетворительной степени доверия

в вопросе приемлемости для получения доступа к такой информации.

3. Лица, получившие разрешение на доступ к информации под грифом НАТО КОНФИДЕНЦИАЛЬНО (NC) или выше, должны получить также соответствующую категорию допуска к секретной информации НАТО (PSC), выданную национальным органом безопасности (NSA) своей страны или другим компетентным органом, и имеющим силу на весь период действия выданного допуска к секретной информации, а также в соответствии с принципом служебной необходимости. Степень процедур по присвоению категории допуска определяется категорией секретности информации НАТО, к которой будет допущено лицо. Процедуры по присвоению категории допуска проводятся в соответствии с политикой безопасности НАТО и соответствующими инструкциями.

4. Лица, получившие разрешение на доступ к информации под грифом НАТО КОНФИДЕНЦИАЛЬНО (NC) или выше, должны получить также соответствующую категорию допуска (PSC), получить инструктаж по процедурам безопасности НАТО, понимать свои обязанности и принцип служебной необходимости. Лица, которым требуется допуск к информации под грифом НАТО - ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ (NR), должны быть проинструктированы по своим обязанностям по безопасности и понимать принцип служебной необходимости. Допуск к секретности не требуется для получения доступа к информации под грифом НАТО - ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ (NR), если не оговорено иное национальными правилами и положениями.

5. Присвоение категории допуска секретности (PSC) не должно расцениваться как завершающий шаг в процессе безопасности персонала; существует требование для гарантирования постоянной приемлемости индивида для получения доступа к секретной информации НАТО. Это достигается через постоянную оценку органами безопасности и руководителями; и через программу обучения и компетентности в области вопросов безопасности, которые напоминают индивидам об их обязанностях в этой области и о необходимости докладывать своим руководителям или персоналу по безопасности об информации, которая может повлиять на статус безопасности.

ПРИМЕНЕНИЕ ПРИНЦИПА СЛУЖЕБНОЙ НЕОБХОДИМОСТИ

6. Лица в странах НАТО и военных и гражданских органах НАТО должны иметь доступ к секретной информации НАТО только на основании принципа служебной необходимости. Ни один индивид не наделяется правом только по званию или должности или категории допуска получить доступ к секретной информации НАТО.

ДОПУСК ПЕРСОНАЛА К СЕКРЕТНОЙ ИНФОРМАЦИИ (PSCs)

Обязанности

7. Обязанности по допуску персонала к секретной информации национальных органов безопасности (NSA) или других компетентных национальных органов государств-членов НАТО, а также и глав гражданских и военных органов НАТО изложены в соответствующей инструкции по безопасности персонала.

8. Индивиды должны осознавать свои обязанности в соответствии с положениями безопасности и действовать в интересах безопасности.

Инструкция по безопасности персонала

9. Соответствующая инструкция по безопасности персонала включает в себя следующее:

(a) требования по определению должностей, требующих соответствующую категорию допуска секретности (PSC);

(b) критерии оценки лояльности, надежности и достоверности в отношении индивида в целях получения им допуска секретности (PSC) и его сохранения;

(c) требования по проведению проверочных мероприятий для получения допуска к информации под грифом НАТО - ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ, НАТО СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО;

(d) требования по обеспечению допуска персонала к секретной информации (PSC) для работников гражданских и военных органов НАТО;

(e) требования по возобновлению действия допуска персонала к секретной информации (PSC);

(f) процедуры по обращению к неблагоприятной информации в отношении лица, обладающего допуском секретности (PSC); и

(g) требования по сохранению данных о лицах, имеющих допуск секретности (PSC).

ОСВЕДОМЛЕННОСТЬ О БЕЗОПАСНОСТИ И ИНСТРУКТАЖ ИНДИВИДОВ

10. Все лица, занимающие должности с наличием допуска к информации под грифом НАТО - для ограниченного пользования, либо имеющие категорию для получения доступа к информации НАТО - КОНФИДЕНЦИАЛЬНО или выше, должны быть проинструктированы по процедурам безопасности и их обязанностям по безопасности. Все лица, получившие допуск, должны подтвердить, что они полностью понимают свои обязанности и последствия, к которым приводит передача информации в несанкционированные руки преднамеренно или вследствие невнимательности, и мероприятия, которые проводятся в соответствии с законом или через административное или исполнительное распоряжение. Подписанный документ-подтверждение должен храниться в базе данных государством-членом НАТО

или гражданским или военным органом НАТО, выдающим допуск к секретной информации НАТО.

11. Все лица, получившие доступ, либо которым требуется работать с секретной информацией НАТО, должны быть осведомлены, а также им необходимо периодически напоминать об опасностях, грозящих безопасности, возникающих из неосторожных разговоров с лицами, для которых в соответствии с принципом служебной необходимости, знание и владение информацией не требуется для выполнения официальных задач и обязанностей, имеющих связи со средствами массовой информации; и об угрозе, которую представляет деятельность спецслужб, для которых целью является НАТО и ее государства-члены. Индивиды должны получить полный инструктаж по этим опасностям и немедленно докладывать соответствующим органам безопасности о каких-либо действиях или попытках, которые они посчитают подозрительными или необычными.

ПРЕДОСТАВЛЕНИЕ ДОСТУПА К СЕКРЕТНОЙ ИНФОРМАЦИИ НАТО

12. Индивид может получить доступ к секретной информации НАТО только после того, как он прошел соответствующую персональную проверку, и была определена служебная необходимость, и он прошел инструктаж по процедурам безопасности НАТО и осознал свои обязанности по безопасности.

Особые обстоятельства

13. Однако могут возникать обстоятельства, когда, например, в целях срочного выполнения задания, некоторые требования из параграфа 12 выше не могут быть выполнены. Подробные данные в отношении временного назначения, единовременного доступа, срочного доступа и посещения конференций и собраний изложены в соответствующей инструкции по безопасности персонала.

ДОСТУП ДЛЯ ЛИЦ, НЕ ЯВЛЯЮЩИХСЯ ГРАЖДАНАМИ ГОСУДАРСТВ-ЧЛЕНОВ НАТО

Доступ для интегрированных членов вооруженных сил государств-членов НАТО

14. Граждане государств, не являющихся членами НАТО, работающие в качестве интегрированных членов вооруженных сил государств-членов НАТО, могут получить разрешение на доступ к информации под грифом СОВЕРШЕННО СЕКРЕТНО. В таких случаях, на национальный орган безопасности возлагается ответственность за соблюдение условий, изложенных в параграфах 12 или 13 выше.

Доступ в поддержку Проекта/программы, контракта, операции НАТО или соответствующей миссии

15. Лица, являющиеся подданными государств, не входящих в состав НАТО[2], могут получать доступ к секретной информации НАТО на основе каждого конкретного случая при условии, что:

(a) доступ необходим в поддержку особой программы, проекта, контракта, операции НАТО или соответствующей миссии;

(b) индивиду была выдана категория допуска секретности НАТО на основании процедуры по присвоению допуска, не менее строгой, чем той, которая требуется для подданного государства-члена НАТО в соответствии с политикой безопасности НАТО и поддерживающих инструкций; с принятием во внимание, что категория допуска секретности НАТО не требуется для доступа к информации под грифом НАТО - ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ; и

(c) было получено предварительное письменное согласие государства-члена НАТО либо гражданского или военного органа, от которого исходила информация.

16. В качестве исключения из требования для контроля источником в подпараграфе 15(c) национальный орган безопасности государств-членов НАТО может одобрить доступ к секретной информации НАТО для граждан определенных государств, не являющихся членами НАТО, которые были наняты на работу правительством страны-члена НАТО либо подрядчиком, который находится и работает в государстве НАТО, при условии, что в дополнение к критериям, перечисленным в подпункте 15(a) и 15(b) выше, применяются критерии, изложенные в эквивалентном разделе соответствующей инструкции по безопасности персонала.

---

[2] Граждане стран, не являющихся членами НАТО включают в себя "подданных Королевства", "граждан Штатов" и "осевшие иммигранты в Канаде". "Осевшие иммигранты в Канаде" - это лица, которые прошли национальную проверку, включая проверку местожительства, сведений о судимости и проверку безопасности, и которые собираются получить законное разрешение на постоянное местожительство в стране.

ПРИЛОЖЕНИЕ "D"
ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ВВЕДЕНИЕ

1. Настоящее Приложение четко излагает политику и минимальные стандарты мер физической безопасности по защите секретной информации НАТО. Подробные данные

находятся в соответствующей инструкции по физической безопасности.

2. Страны-члены НАТО и военные и гражданские органы НАТО должны создать программы физической безопасности, удовлетворяющие этим минимальным стандартам. Такие программы, состоящие как из активных, так и пассивных мер по безопасности, должны обеспечивать общий уровень защиты в соответствии с классификацией безопасности защищаемой секретной информации НАТО.

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

3. Все помещения, здания, офисы, комнаты и другие районы в которых хранится и/или обращается секретная информация и материалы НАТО, должны быть защищены соответствующими мерами по физической безопасности. При решении, какая степень защиты по физической безопасности необходима, нужно учитывать все имеющие к этому отношение факторы, такие как:

(a) уровень секретности и категория информации;

(b) количество и форма располагаемой информации (печатный текст/хранящаяся на компьютере);

(c) допуск к секретной информации и принцип служебной необходимости по допуску персонала к секретной информации;

(d) оценка на местности угрозы от служб разведок, имеющих своей целью НАТО и/или страны-члены НАТО, диверсия, терроризм, подрывные или криминальные действия; и

(e) как информация будет храниться.

4. Меры физической безопасности должны быть разработаны по:

(a) препятствию тайному или силовому вторжению нарушителя;

(b) удерживанию, препятствованию и обнаружению действий неблагонадежных лиц (шпионов изнутри);

(c) разделению персонала в их допуске к секретной информации НАТО в соответствии с принципом служебной необходимости; и

(d) обнаружению и действию по всем нарушениям безопасности в кратчайшие сроки.

МЕРЫ ПО ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

5. Физические меры представляют только один аспект обеспечения безопасности и должны быть поддержаны озвучиванием безопасности персонала, безопасностью информации и мерами по информационной безопасности, детали которых находятся в Приложениях "C", "E" и "F", соответственно. Практическая организация безопасности против риска включает установление наиболее действенных и рентабельных методов противодействия угрозам и уравновешивающих уязвимость комбинации мер по защите

от таких областей риска. Наиболее лучшим образом такая действенность и рентабельность достигается определением требований по физической безопасности как части планирования и разработки инфраструктуры, таким образом, уменьшая необходимость для дорогостоящей реконструкции.

6. Программы физической безопасности должны основываться на принципе " глубокая оборона", и хотя меры физической безопасности зависят от места, следующие принципы должны применяться. Во-первых, необходимо определить помещения, требующие защиты. Затем принимаются меры многоуровневой защиты для обеспечения "глубокой обороны" и факторы задержки. Самые внешние меры физической защиты должны определять район защиты и удержать от несанкционированного доступа. Следующий уровень мер должен определить несанкционированный доступ или попытку доступа и привести в состояние готовности силы охраны. Самый внутренний уровень мер должен быть достаточным для задержки нарушителей до момента, когда они могут быть взяты под стражу силами охраны. Поэтому, существует взаимная связь между временем реакции сил охраны и мерами физической безопасности, разработанными для задержки нарушителя.

7. Регулярное обслуживание систем физической безопасности необходимо для гарантированного функционирования оборудования с оптимальными характеристиками. Также необходимо периодически производить переоценку эффективности мер индивидуальной безопасности и системы безопасности в целом. Это может быть достигнуто путем тренировки выполнения плана ответных действий.

Районы безопасности

8. Районы, в которых информация с грифом секретности НАТО КОНФИДЕНЦИАЛЬНО (NC) и выше обращается и хранится, должны быть организованы и систематизированы в соответствии с одним из следующих требований:

(a) **Район безопасности НАТО класса** I район, в котором секретная информация с грифом НАТО КОНФИДЕНЦИАЛЬНО (NC) и выше обращается и хранится таким образом, что вход в район со всеми возможными намерениями создает доступ к секретной информации. Такие районы требуют:

(i) четкого определенного и защищаемого периметра, через который контролируются все входы и выходы;

(ii) системы контроля за доступом, которая позволяет иметь доступ только лицам, имеющим соответствующий доступ и особую санкцию на вход в район;

(iii) спецификации уровня секретности и категории информации, обычно обращаемой в районе, то есть информации, к которой вход дает доступ;

(b) **Район безопасности НАТО класса** II район, в котором секретная информация с грифом НАТО КОНФИДЕНЦИАЛЬНО (NC) и выше обращается и хранится таким

образом, что может быть защищена от несанкционированного доступа посредством мер внутреннего контроля. Такие районы требуют:

(i) четкого определенного и защищаемого периметра, через который контролируются все входы и выходы;

(ii) системы контроля за доступом, позволяющую иметь доступ без сопровождения только лицам, поверенным на благонадежность и имеющим специальное разрешение на вход в район. Для других лиц предоставление допуска должно осуществляться с сопровождением или эквивалентным контролем для предотвращения несанкционированного допуска к секретной информации НАТО и неконтролируемого входа в район, являющийся предметом проверки технической безопасности.

9. Те районы, которые не заняты персоналом во время суточного несения службы, после окончания рабочего дня должны быть немедленно проверены с целью гарантирования того, что секретная информация НАТО защищена соответствующим образом.

Административные зоны

10. Административная зона может устанавливаться вокруг или вести к районам безопасности НАТО класса I или класса II. Такая зона требует визуально определяемого периметра, в пределах которого существует возможность контроля персонала и транспортных средств. Только секретная информация с грифом до и включительно "НАТО ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ" (NR) - должна обращаться и храниться в Административных зонах.

Особые меры

11. Следующие меры определены для обозначения примеров мер по физической безопасности, которые могут быть применены:

(a) заграждение (забор) периметра - забор периметра позволит сформировать действенную физическую преграду и будет определять границы требующего защиты района. Эффективность любого периметра безопасности в значительной степени будет зависеть от уровня безопасности в точках допуска;

(b) система обнаружения нарушителя (IDS) - (IDS) может быть использована по периметру для усиления уровня безопасности, предоставляемого заграждением, или может быть использована в помещениях и зданиях вместо или для помощи охране;

(c) контроль допуска - контроль допуска может осуществляться на участке, в здании или зданиях на участке или районе, или помещениях внутри здания. Контроль может быть электронным, электронно-механическим, посредством охранников или лица, ведущего прием посетителей, или физический;

(d) охрана - использование соответствующим образом проверенных на

благонадежность, обученных и контролируемых охранников может создать значительное препятствие для лиц, имеющих план скрытого проникновения;

(e) система скрытого наблюдения (CCTV) - (CCTV) это ценная помощь охране в проверке инцидентов и тревоги системы обнаружения нарушителя (IDS) на больших участках или периметрах; и

(f) освещение безопасности - освещение безопасности может предоставить высокую степень препятствия для проникновения нарушителя, в дополнения обеспечения освещением, необходимым для осуществления эффективного наблюдения, непосредственно персоналом охраны либо посредством системы скрытого наблюдения.

Осмотр на входе и выходе

12. Учреждения НАТО должны предпринимать случайные проверки на входе и выходе, предназначенные в качестве действий по препятствованию несанкционированного вноса и выноса из места или здания материалов и секретной информации.

Контроль доступа

13. Пропуск или система распознавания, контролирующая штатный персонал, должна контролировать доступ в районы с уровнем безопасности класса I и класса II. Посетителям должен быть разрешен доступ (в сопровождении или без сопровождения) в учреждения НАТО, основываясь на проверке личности и регламентов на их допуск.

МИНИМАЛЬНЫЕ СТАНДАРТЫ ХРАНЕНИЯ СЕКРЕТНОЙ ИНФОРМАЦИИ НАТО

14. Секретная информация НАТО должна храниться только при условиях, разработанных для препятствования несанкционированного допуска к информации.

15. **СОВЕРШЕННО СЕКРЕТНО (CTS).** Информации с грифом "CTS" должна храниться в районах с уровнем безопасности класса I и класса II при следующих условиях:

(a) в сейфе, оборудованном системой обнаружения нарушителя (IDS) или в безопасном контейнере, одобренном страной, в районе, который является предметом постоянной защиты или периодической проверки; и

(b) в оборудованном системой обнаружения нарушителя (IDS) открытом районе хранения в соответствии с инструкциями, обеспечивающими физическую защиту.

16. **НАТО СЕКРЕТНО (NS).** Информации с грифом "NS" должна храниться в районах с уровнем безопасности класса I и класса II при следующих условиях:

(a) в таких же условиях, как предписано для информации с грифом (CTS); или

(b) в одобренном страной безопасном контейнере или сейфе; или

(c) в открытом районе хранения, оборудованном системой обнаружения нарушителя (IDS), или в регионе который является предметом постоянной защиты или периодической проверки.

17. **НАТО КОНФИДЕНЦИАЛЬНО (NC).** Информация с грифом "NC" должна храниться в таких же условиях, как предписано для информации с грифом (CTS) или (NS), за исключением той, которая не требует дополнительных мер контроля, описанных в инструкциях по обеспечению физической безопасности.

18. **НАТО ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ (NR).** Информация с грифом "NR" должна храниться в закрытых контейнерах.

19. Расширенные детали по хранению секретной информации НАТО изложены в соответствующих инструкциях по физической безопасности.

ЗАЩИТА ОТ ТЕХНИЧЕСКИХ СРЕДСТВ ПО ПЕРЕХВАТУ ИНФОРМАЦИИ

Несанкционированное извлечение информации

20. Офисы или зоны, в которых регулярно обсуждается секретная информация с грифом НАТО СЕКРЕТНО (NS) и выше, должны быть защищены против активных и пассивных несанкционированных извлечений посредством принятия мер звуковой физической защиты и контроля доступа в места возможного риска по осуществлению таких действий. Ответственность по определению риска должна быть согласована с техническими специалистами, и решение должно быть принято соответствующим руководством по безопасности.

Технически безопасные районы

21. Зоны, защищаемые против несанкционированного извлечения аудио информации, должны определяться как районы технически безопасные, и вход в такие районы должен особо контролироваться. Помещения, в которых не проводится работа, должны быть закрыты на замки и/или охраняться в соответствии со стандартами физической безопасности, а любые ключи рассматриваются как ключи системы защиты. Такие зоны будут являться предметом регулярных физических и/или технических инспекций в соответствии с требованиями соответствующего руководства по безопасности, которые также будут предприниматься после любого несанкционированного проникновения или подозрений о таком проникновении и входа персонала для проведения работ по обслуживанию или ремонту помещений.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ СИСТЕМ СВЯЗИ И ИНФОРМАЦИИ (CIS)

22. Зоны, в которых секретная информация НАТО представляется или обращается, используя информационные технологии, или где возможен потенциальный доступ к такой информации, должны быть организованы с выполнением совокупных требований по конфиденциальности, целостности и наличию информации. Зоны, в которых располагается, хранится, обрабатывается или передается секретная информация с грифом "НАТО СЕКРЕТНО" (NS) и выше, или где возможен потенциальный доступ к такой информации, должны быть организованы как зоны с уровнем безопасности НАТО класса I и класса II или национальным эквивалентом уровня безопасности. Районы, в которых располагается, хранится, обрабатывается или передается секретная информация с грифом "NR" или где возможен потенциальный доступ к такой информации, могут быть организованы как Административные зоны.

САНКЦИОНИРОВАННОЕ ОБОРУДОВАНИЕ

23. Национальный орган безопасности (NSA) должен вести списки оборудования, которое они или другие страны-члены НАТО санкционировали на использование для защиты секретной информации НАТО при различных указанных обстоятельствах и условиях. Военные и гражданские органы НАТО должны гарантировать, что любое покупаемое оборудование соответствует Положениям (правилам) стран(ы)-член(а)ов НАТО.

ДРУГИЕ МЕРЫ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

24. Детальные требования изложены в соответствующих инструкциях по обеспечению физической безопасности в отношении, например, помещений и замков, ключей и комбинации кодов, контейнеров и замков.

ПРИЛОЖЕНИЕ "E"
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ВВЕДЕНИЕ

1. Настоящее Приложение излагает политику и минимальные стандарты защиты секретной информации НАТО. Подробные данные находятся в соответствующей инструкции по безопасности информации.

2. Секретная информация НАТО требует защиты в течение всего своего существования. С информацией необходимо обращаться так, чтобы гарантировать ее соответствующую секретность, четкую идентификацию в качестве секретной информации и пребывание ее таковой только в течение необходимого периода. Меры по обеспечению безопасности информации должны дополняться персоналом,

физической защитой и защитой информационной безопасности в целях обеспечения сбалансированного ряда мер для защиты секретной информации НАТО.

ГРИФ СЕКРЕТНОСТИ И МАРКИРОВКИ

Общая часть

3. Составитель несет ответственность за определение грифа секретности и первоначальное распространение информации. Уровень секретности информации НАТО не должен быть изменен, понижен или отменен без согласия составителя. Приготовляя информацию, составитель должен указать, где это возможно, определенную дату или событие, при которых информация может быть понижена в грифе секретности или рассекречена.

4. Присвоенный гриф секретности определяет физическую безопасность по хранению и передаче информации, ее циркуляции и уничтожения и требования по проверке на благонадежность персонала для получения допуска к информации. Вследствие этого, в интересах эффективности и действенности безопасности необходимо равным образом избегать как завышения, так и занижения грифа секретности.

5. Страны-члены НАТО и военные и гражданские органы НАТО должны внедрять меры, гарантирующие, что информация, составленная НАТО или предназначенная для НАТО, имеет надлежащий гриф секретности и защищена в соответствии с требованиями соответствующих инструкций по безопасности информации.

6. Каждый военный и гражданский орган НАТО должен установить систему, обеспечивающую просмотр составленной им информации с грифом "СОВЕРШЕННО СЕКРЕТНО" (CTS) не реже одного раза в пять лет на предмет определения целесообразности сохранения грифа "СОВЕРШЕННО СЕКРЕТНО" (CTS). Такой обзор не обязателен для тех инстанций, в которых составитель информации предопределил, что особая информация с грифом "СОВЕРШЕННО СЕКРЕТНО" (CTS) должна автоматически понижаться в грифе секретности по истечении двух лет, и такая информация имеет соответствующую маркировку.

7. Общий уровень секретности документа должен быть, по крайней мере, таким же, какой имеет наиболее секретный компонент. Части документа, имеющие гриф секретности "НАТО КОНФИДЕНЦИАЛЬНО" (NC) и выше, должны, где возможно, быть засекречены составителем (включая параграф) для упрощения решения по дальнейшему распространению соответствующей части. Сопроводительные документы должны быть отмечены грифом секретности информации, содержащейся в них, при ее отделении от той информации, которую они сопровождают.

8. При сопоставлении информации, полученной из разных источников, должен

быть проверен общий уровень секретности документа, так как он может потребовать более высокого грифа секретности, чем отдельные его компоненты. При использовании информации для подготовки составного документа должны быть напомнены пояснения о общем уровне секретности.

Маркировки категории

9. Обозначения "COSMIC" и "НАТО" являются маркировками категорий, которые применяются к секретной информации, обозначающими, что информация должна быть защищена в соответствие с Политикой безопасности НАТО.

Указатели специальной категории

10. Обозначение "ATOMAL" - маркировка, применяемая к информации специальной категории, обозначающей, что информация должна быть защищена в соответствии с Приложением "B", параграф 5.

11. Обозначение "SIOP" - маркировка, применяемая к информации специальной категории, обозначающей, что информация должна быть защищена в соответствии со ссылкой, упомянутой в Приложении "B", параграф 6.

12. Обозначение "CRYPTO" - маркировка и указатель специальной категории, определяющей все ключевые материалы "COMSEC", используемые для защиты или установления подлинности средств связи, передающих информацию НАТО, имеющую отношение к безопасности; определяет, что информация должна быть защищена в соответствии с инструкциями по криптографической безопасности.

Указатели ограничения распространения

13. Как дополнительный указатель к дальнейшему ограничению распространения секретной информации НАТО составителем может применяться указатель ограничения распространения.

КОНТРОЛЬ И ОБРАЩЕНИЕ

Задачи отчетности

14. Первостепенной задачей отчетности является обеспечение достаточной информацией для проведения расследования преднамеренной или случайной компрометации отчетной информации и оценки возникшего в этой связи урона. Требования по отчетности служат установлению дисциплины при обращении с подотчетной информацией и для контроля допуска к ней.

15. Второстепенными задачами являются:

(a) отслеживать доступ к подотчетной информации, кто имеет или потенциально имеет, имел доступ к подотчетной информации; и кто пытался иметь доступ к подотчетной информации;

(b) знать расположение подотчетной информации; и

(c) отслеживать циркуляцию подотчетной информации в пределах НАТО территориях стран.

16. Информация с грифом "COSMIC", "NC" и "ATOMAL" должна быть подотчетной, контролируемой и обращаемой в соответствии с требованиями настоящего Приложения и соответствующих инструкций по безопасности информации. Где требуют национальные правила и положения, информация, несущая другой гриф секретности или с указателями специальной категории, может рассматриваться в качестве подотчетной информации.

Система регистрации

17. Должна существовать система регистрации, отвечающая за прием, ведение учета, обращение и уничтожение подотчетной информации. Такое обязательство может выполняться либо в пределах одной системы регистрации, в которой информация с грифом (CTS) должна постоянно строго категорироваться или для нее должны быть установлены отдельные пункты регистрации и контроле.

18. Каждая страна-член НАТО и военные и гражданские организации НАТО должны установить Центральную канцелярию (и) для информации с грифом "*CTS*", действующую как основной национальный орган власти или орган власти, в пределах которого он установлен, получающий и отправляющий информацию. Центральная канцелярия может также действовать в качестве регистрационного пункта(ов) для другой подотчетной информации.

19. Канцелярии и пункты регистрации должны действовать как ответственные организации по внутреннему распространению секретной информации с грифом " СОВЕРШЕННО СЕКРЕТНО" (*CTS*) и "НАТО СЕКРЕТНО" (*NS*) и ведению записей по всем подотчетным документам, находящимся под контролем этих регистрационных пунктов; они могут быть организованы в министерстве, департаменте или на командном уровне. Информация с грифом "НАТО КОНФИДЕНЦИАЛЬНО" (*NS*) и " НАТО ДЛЯ ОГРАНИЧЕННОГО ПОЛЬЗОВАНИЯ" (*NR*) не обязательна к обработке через систему регистрации, кроме случаев, оговоренных национальными правилами и положениями.

20. Канцелярии и пункты регистрации должны быть способными в любое время определить местонахождение подотчетной информации НАТО. Нечастый и временный допуск к такой информации не требует обязательного учреждения канцелярии или

пункта регистрации при условии, что процедуры на месте гарантируют, что информация останется под контролем системы регистрации.

21. Распространение секретной информации с грифом "СОВЕРШЕННО СЕКРЕТНО" (*CTS*) должно осуществляться через регистрационные каналы *COSMIC*. Не реже одного раза в год каждый регистрационный пункт (канцелярия) должен производить инвентаризацию всей секретной информации с грифом "*CTS*", являющей подотчетной в соответствии с требованиями соответствующих инструкций по безопасности информации. Независимо от вида организации регистра, персонал, работающий с информацией с грифом "*CTS*" должен быть допущен офицером по контролю за совершенно секретной информацией (*COSMIC Control Officer* (*CCO*).

22. Соответствующие инструкции по безопасности информации, кроме прочего, устанавливают обязанности офицера по контролю за совершенно секретной информацией (*COSMIC Control Officer* (*CCO*), детальные процессы обращения с секретной информацией с грифом "СОВЕРШЕННО СЕКРЕТНО" (*CTS*) и "НАТО СЕКРЕТНО" (*NS*), системой регистрации, процедуры размножения, перевода и выписок, требований по распространению или передаче информации, и требований по устранению и уничтожению информации.

23. Военный комитет НАТО установил раздельные системы для отчетности, контроля и распространения секретных материалов. Материалы, распространяемые посредством этих систем, не требуют подотчетности в системе регистрации.

ПЛАНИРОВАНИЕ НА СЛУЧАЙ ЧРЕЗВЫЧАЙНЫХ ОБСТОЯТЕЛЬСТВ

24. Страны-члены НАТО и военные и гражданские организации НАТО должны подготовить план действий при чрезвычайных ситуациях по защите или уничтожению во время чрезвычайных обстоятельств секретной информации НАТО в целях предотвращения несанкционированного доступа и разглашения и потери наличия. Наивысший приоритет в этих планах должен быть отдан наиболее чувствительной, оперативной и ограниченной по времени информации.

НАРУШЕНИЕ БЕЗОПАСНОСТИ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП И НЕСАНКЦИОНИРОВАННОЕ РАЗГЛАШЕНИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

25. Защита секретной информации НАТО зависит от лежащих в основе соответствующих инструкций по безопасности, приводящих в исполнение утвержденные политику, директивы и руководства, и от эффективной реализации этих инструкций путем обучения и контроля совместно с дисциплинарными взысканиями и правовыми санкциями в экстремальных случаях.

26. Обо всех нарушениях безопасности должно незамедлительно докладываться

соответствующему руководству по безопасности. Каждый случай нарушения безопасности должен быть расследован лицами, имеющими соответствующий опыт в области безопасности, проведения расследований и контрразведывательной деятельности, а также независимыми от лиц имеющих отношение к нарушению.

27. Основной целью доклада о несанкционированном доступе к секретной информации НАТО является содействие компоненту НАТО, составившему информацию, оценить результаты причиненного ущерба НАТО и принятие каких-либо необходимых или практических действий по уменьшению такого ущерба. Рапорт об оценке ущерба и действиях по его уменьшению должен быть передан в Офис безопасности НАТО (*NOS*).

28. После доклада о несанкционированном доступе к секретной информации НАТО в Офис безопасности НАТО (*NOS*), рапорт должен быть передан в национальный орган безопасности (*NSA*) и Главе военного и гражданского органа НАТО в части их касающейся. Когда это возможно, руководство, которому докладывают, должно одновременно информировать компонент НАТО, составивший информацию и Офис безопасности НАТО (*NOS*), но последняя из названных инстанций может потребовать это сделать в том случае, когда трудно определить составителя. Время подачи рапортов зависит от характера информации и обстоятельств.

29. Генеральный Секретарь НАТО может потребовать соответствующие власти провести дальнейшее расследование и доложить о его результатах.

30. Соответствующие инструкции по безопасности устанавливают подробные действия, записи и требования относительно докладов о нарушении и несанкционированном доступе.

31. Отдельные положения, имеющие отношение к несанкционированному доступу к криптографическим материалам, выдаются Военным командованием НАТО, руководству по безопасности связи и странам-членам НАТО и военным и гражданским организациям НАТО.

МЕРОПРИЯТИЯ БЕЗОПАСНОСТИ ПО РАЗРЕШЕНИЮ НА ПЕРЕДАЧУ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИИ НАТО СТРАНАМ НЕ ЯВЛЯЮЩИМСЯ ЧЛЕНАМИ НАТО, И МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

Введение

32. Классифицированная информация, вверенная или составленная НАТО в целях способствования выполнения задач НАТО, распространяется и защищается в соответствии с Политикой безопасности НАТО, директивами и процедурами. Этот

параграф устанавливает политику по разрешению на передачу классифицированной информации НАТО странам не являющимся членами НАТО, и международным организациям, включая такие страны (в дальнейшем именуемые как получатели - не члены НАТО). Параграф также затрагивает информацию, содержащуюся в документах, выпущенных Североатлантическим Советом (*NAC*) или любым другим комитетом НАТО или военным или гражданским органом (в дальнейшем именуемые как органы НАТО).

33. Передача секретной информации НАТО получателям - не членам НАТО, должна осуществляться в контексте сотрудничества НАТО, утвержденного Североатлантическим Советом (NAC).

34. Информация любой классификации касательно ядерного оружия "*ATOMAL*" не может передаваться любой стране/организации, которые не являются участниками существующей версии *C-M(64)39* и *C-M(68)41*.

ПРИНЦИПЫ САНКЦИОНИРОВАНИЯ ПЕРЕДАЧИ СЕКРЕТНОЙ ИНФОРМАЦИИ НАТО ДО СТРАН НЕ ЯВЛЯЮЩИХСЯ ЧЛЕНАМИ НАТО И МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

35. Санкционирование передачи информации всегда должно быть предметом согласия составителя информации. Кроме того, должны быть соблюдены следующие требования:

(a) для классифицированной информации, распространяемой в рамках мероприятий НАТО по сотрудничеству, утвержденному Североатлантическим Советом (NAC):

(i) предмет обсуждения должен быть включен в общий рабочий план мероприятий или в практические установленные меры по сотрудничеству;

(ii) передача классифицированной информации НАТО должна быть затребована для начала сотрудничества по особой тематике или для продолжения и дальнейшего развития сотрудничества в утвержденных рамках; и

(iii) должно быть заключено Соглашение по безопасности, подписанное Генеральным секретарем от имени НАТО и уполномоченным представителем страны, не являющейся членом НАТО - получателем информации;

(b) для секретной информации НАТО, передаваемой по особому запросу со стороны либо НАТО, либо страны-члена НАТО или органов НАТО (Инициатор) стране , не являющейся членом НАТО, вне рамок мероприятий НАТО по сотрудничеству, утвержденному Североатлантическим Советом (NAC):

(i) Инициатор несет ответственность за предоставление НАТО письменной гарантии от получателя информации, не являющегося членом НАТО, что полученная информация будет защищена в соответствии с минимальными стандартами НАТО.

(ii) Инициатор должен передать эту подписанную гарантию соответствующим

комитетам вместе с запросом на доведение информации; и

(iii) запрос должен демонстрировать преимущества, которые могут быть приобретены НАТО в этой связи. Обоснование допуска должно быть точным, избегая общих формулировок.

36. Выдача разрешений, сделанных в соответствии с параграфом 35(a) выше, может касаться либо четко определенной информации, либо информации общей категории. Выдача разрешений, сделанных в соответствии с параграфом 35(b), может касаться только четко определенной информации.

Руководство по безопасности

37. Североатлантический Совет (*NAC*) является высшей властью, санкционирующей доведение секретной информации НАТО получателям, не являющимся членами НАТО. Такие полномочия должны соблюдать принцип одобрения составителя информации и передаются:

(a) соответствующим комитетам для информации, классифицированной как "НАТО КОНФЕДИЦИАЛЬНО" (*NC*) и выше.

(b) Военному комитету НАТО (*NAMILCOM*) для информации, классифицированной как "НАТО СЕКРЕТНО" (*NS*) и выше, составленную Военным комитетом НАТО (*NAMILCOM*) и подчиненными ему органами.

(c) организации НАТО по производству и тыловому обеспечению (*NPLO*) для классифицированной информации НАТО, составленной или принадлежащей одной (или более) стране-члену организации НАТО по производству и тыловому обеспечению (*NPLO*).

38. Полномочиями на передачу информации должен быть наделен только комитет, представитель которого составил информацию. Если составитель не может быть установлен, соответствующий комитет должен взять на себя обязанности составителя. Полномочиями на передачу информации может быть наделен самый низкий уровень комитета, который лучше подходит для оценки важности секретной информации.

39. Наделенные полномочиями по передаче не могут в свою очередь предать это право, несмотря на то, что они могут возлагать на подчиненные органы исполнение решения по передаче.

АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ ПО ИСПОЛНЕНИЮ СОГЛАШЕНИЯ ПО БЕЗОПАСНОСТИ

40. Завершение административных мероприятий должно быть подтверждено результатом проверки режима секретности, проводимой Офисом безопасности НАТО соответствующих ведомств получателя информации, не являющегося членом НАТО. Проверка режима секретности должна установить способность получателя информации

, не являющегося членом НАТО, соответствовать требованиям Соглашения о безопасности и минимальным стандартам.

41. Офис безопасности НАТО должен составить отчет о поверке режима секретности и передать копию Руководству по безопасности получателя информации, не являющегося членом НАТО. Оригинал рапорта должен храниться в Офисе безопасности НАТО и быть доступным для стран-членов НАТО. Выводы, сделанные на основании рапорта в отношении способности получателя информации, не являющегося членом НАТО, защищать классифицированную информацию НАТО, должны быть сообщены Офисом безопасности НАТО соответствующим органам НАТО и странам-членам НАТО.

42. Соответствующие инструкции по безопасности информации, наряду с прочим, содержат:

(a) процедуры по передаче секретной информации НАТО получателям, не являющимся членами НАТО;

(b) особые процедуры распространения для Организации НАТО по производству и тыловому обеспечению (*NPLO*), международных организаций и многонациональных объединенных оперативно-тактических групп (*CJTF*);

(c) минимальные стандарты, требуемые для обращения и защиты секретной информации НАТО, доведенной до получателей, не являющихся членами НАТО. Минимальные стандарты, применяемые к любым получателям информации, не членам НАТО, независимо от заключения Соглашения о безопасности с НАТО или предоставления НАТО гарантии по безопасности;

(d) Детальные административные мероприятия, которые должны быть исполнены всеми получателями информации, не являющимися членами НАТО; и

(e) образцы Гарантии безопасности, сертификата о благонадежности личного состава и сертификат о допуске к секретам.

ПРИЛОЖЕНИЕ "F"
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ВВЕДЕНИЕ

1. Настоящее Приложение четко излагает политику и минимальные стандарты защиты классифицированной информации НАТО и поддерживающих системных служб и ресурсов в системах связи, информации и других электронных систем (далее именуемые в настоящем Приложении системами), используемыми для хранения, обработки или передачи (в дальнейшем именуемые в настоящем приложении как обработка) классифицированной информации НАТО.

2. "Главная инструкция информационной безопасности", опубликованная Советом

национальной безопасности и Советом НАТО по консультациям, командованию и управлению (*NC3B*) в поддержку настоящей политики, рассматривает деятельность информационной безопасности в системе жизненного цикла и обязанностей по информационной безопасности комитетов и гражданских и военных органов НАТО. " Главная инструкция Службы информационной безопасности" поддерживается инструкциями по управлению информационной безопасностью (включая управление рисками безопасности, аттестат безопасности, документация, касающаяся безопасности , и обзор/проверка безопасности), техническими аспектами и аспектами реализации информационной безопасности (включая безопасность компьютерной и локальной сети , взаимосвязь безопасности сети, криптографической защиты, скрытности связи и конфиденциальности передачи данных).

Задачи безопасности

3. Для достижения адекватной защиты безопасности классифицированной информации НАТО, обрабатываемой в системах, необходимо определить и реализовать сбалансированный ряд мер безопасности (физических, кадровых, информационных и мер информационной безопасности) для создания безопасной среды, в которой работает система и для выполнения следующих задач безопасности:

(a) для обеспечения конфиденциальности информации путем контролирования разглашения и доступа к секретной информации НАТО и поддерживающим системным службам и ресурсам;

(b) для обеспечения целостности классифицированной информации НАТО и поддерживающих системных служб и ресурсов; и

(c) для обеспечения доступности классифицированной информации НАТО и поддерживающих системных служб и ресурсов.

4. Целостность и доступность классифицированной информации НАТО и поддерживающих системных служб и ресурсов должны быть защищены минимальными мерами, нацеленными на обеспечение общей защиты против обычно встречающихся проблем (как случайных, так и преднамеренных), которые, как известно, оказывают влияние на все системы и поддерживающие системные службы и ресурсы. Должны быть приняты дополнительные меры, соответствующие обстоятельствам, в которых оценкой рисков было установлено, что классифицированная информация НАТО и/или поддерживающие системные службы и ресурсы подвергаются повышенному риску особых угроз и уязвимости.

АТТЕСТАТ БЕЗОПАСНОСТИ

5. Степень реализации задач безопасности и надежности мер информационной безопасности для защиты классифицированной информации НАТО и поддерживающих

системных служб и ресурсов определяется в ходе процесса установления требований безопасности. Процесс аттестации безопасности должен определить был ли достигнут и поддерживается ли адекватный уровень защиты.

6. Все системы, обрабатывающие классифицированную информацию НАТО, должны подвергаться процессу аттестации безопасности с рассмотрением задач безопасности по конфиденциальности, целостности и доступности.

БЕЗОПАСНОСТЬ ПЕРСОНАЛА

7. Лица, получившие доступ к классифицированной информации НАТО любой формы, должны пройти проверку безопасности на соответствующем уровне, принимая во внимание их общие обязанности по соблюдению конфиденциальности, целостности и доступности информации и поддерживающих системных служб и ресурсов. В эту категорию также входят лица, получившие доступ к поддерживающим системным службам и ресурсам, либо те лица, которые отвечают за их защиту, даже если они не имеют доступа к информации, обрабатываемой системой.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

8. Области, в которых представлена и обрабатывается классифицированная информация НАТО с использованием информационных технологий или где возможен потенциальный доступ к такой информации, должны устанавливаться таким образом, чтобы соблюдались основные требования по конфиденциальности, целостности и доступности.

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

9. Все классифицированные компьютерные носители информации должны быть должным образом идентифицированы, храниться и защищаться таким образом, который соответствует наивысшей классификации хранения информации.

10. Классифицированная информация НАТО, записанная на компьютерных носителях многоразового использования, должна стираться только в соответствии с процедурами, одобренными органом безопасности.

ОТВЕТСТВЕННОСТЬ

11. Необходимо наличие средства обеспечения достаточного количества информации для расследования преднамеренной или случайной компрометации конфиденциальности информации и, в соответствии с возможным наносимым ущербом

, преднамеренной или случайной компрометации целостности и/или доступности классифицированной информации НАТО и поддерживающих системных служб и ресурсов.

МЕРЫ БЕЗОПАСНОСТИ

12. Для всех систем, обрабатывающих классифицированную информацию НАТО, необходимо применение последовательного ряда мер безопасности в целях соответствия задачам безопасности и защиты информации и поддерживающих системных служб и ресурсов. Меры безопасности должны включать следующее:

(a) способ надежно определить и установить подлинность лиц, имеющих разрешение на доступ. Информация и материал, контролирующий доступ к системе, должны проверяться и защищаться мероприятиями, соответствующими информации, к которой может быть получен доступ;

(b) способ контроля за разглашением и получением доступа к информации и поддерживающим системным службам и ресурсам, на основании принципа служебного соответствия;

(c) способ проверки целостности и источника информации и поддерживающих системных служб и ресурсов;

(d) способ поддержания целостности классифицированной информации НАТО и поддерживающих системных служб и ресурсов;

(e) способ поддержания доступности классифицированной информации НАТО и поддерживающих системных служб и ресурсов;

(f) способ контролирования связи систем, обрабатывающих классифицированную информацию НАТО;

(g) определение уверенности в защитных механизмах информационной безопасности;

(h) способ оценивания и проверки правильного функционирования защитных механизмов информационной безопасности в течение жизненного цикла системы; и

(i) способ расследования деятельности системы и пользователя.

13. Механизмы и процедуры управления безопасностью должны быть приняты для удержания, предупреждения, обнаружения и восстановления после воздействия инцидентов, влияющих на конфиденциальность, целостность и доступность классифицированной информации НАТО и поддерживающих системных служб и ресурсов, включая доклад об инцидентах в области безопасности.

14. Меры безопасности должны регулироваться и реализовываться в соответствии с инструкциями, поддерживающими эту политику.

УПРАВЛЕНИЕ РИСКАМИ В ОБЛАСТИ БЕЗОПАСНОСТИ

15. Системы, обрабатывающие классифицированную информацию НАТО в гражданских и военных органах НАТО, должны подвергаться оценке риска и управлению риском в соответствии с требованиями инструкций, поддерживающих эту политику.

ЭЛЕКТРОМАГНИТНАЯ ПЕРЕДАЧА СЕКРЕТНОЙ ИНФОРМАЦИИ НАТО

16. Когда секретная информация НАТО передается электромагнитным путем, необходимо принять специальные меры для защиты конфиденциальности, целостности и доступности такой передачи. Органы НАТО должны определить требования по защите передачи от обнаружения, перехвата или использования. Информация, передающаяся в системах связи, должна быть защищена на основании требований о конфиденциальности, целостности и доступности.

17. Когда для обеспечения защиты конфиденциальности, целостности и доступности требуются криптографические методы, такие методы или сопутствующие продукты должны быть специально одобрены для этой цели.

18. Во время передачи конфиденциальность информации под грифом "НАТО СЕКРЕТНО" (*NS*) и выше должна обеспечиваться защитой криптографическими методами или продуктами, одобренными военным комитетом НАТО (*NAMILCOM*).

19. Во время передачи конфиденциальность информации, классифицированной как "НАТО - конфиденциально" или "НАТО - для ограниченного пользования" должна охраняться криптографическими методами или продуктами, одобренными военным комитетом НАТО или государством-членом НАТО, за исключением случая, когда метод или продукт финансируется НАТО, когда одобрение быть получено военным комитетом НАТО (*NAMILCOM*).

20. Во время передачи целостность и доступность классифицированной информации должна удостоверяться в соответствии с оперативными требованиями системы связи. Требования оценки и орган одобрения должны быть определены и согласованы в соответствии со спецификацией таких механизмов в оперативных требованиях, как оговорено в технических инструкциях.

21. При исключительных оперативных обстоятельствах информация классифицирующаяся как "НАТО - конфиденциально", "НАТО - для ограниченного пользования" и "НАТО СЕКРЕТНО" может передаваться открытым текстом при условии, что каждый подобный случай разрешен. Исключительные обстоятельства могут быть следующими:

a) во время надвигающегося или действительного кризиса, конфликта или военной ситуации; и

(b) когда скорость доставки имеет огромное значение или средства шифрования недоступны, и было определено, что передаваемая информация не может быть

использована вовремя и неблагоприятно повлияет на операцию.

22. Во время передачи в пределах систем государств, не являющихся членами НАТО/Международных организаций, конфиденциальность информации под грифом НАТО СЕКРЕТНО и выше должна защищаться криптографическими методами или продуктами, одобренными военным комитетом НАТО. Во время передачи в пределах систем государств, не являющихся членами НАТО/Международных организаций, конфиденциальность информации под грифом "НАТО - конфиденциально" или "НАТО - для ограниченного пользования" должна обеспечиваться криптографическими методами или продуктами, оцениваемыми или одобренными соответствующим органом. Соответствующим органом может являться военный комитет НАТО, Национальный орган безопасности связи государства-члена НАТО или эквивалентный орган государств, не являющихся членами НАТО/Международных организаций, при условии, что последние имеют структуры, правила и процедуры для оценки, отбора, одобрения и контроля таких методов или продуктов. Структуры, правила и процедуры должны согласовываться между НАТО и государствами, не являющимися членами НАТО/Международных организаций.

БЕЗОПАСНОСТЬ КРИПТОГРАФИЧЕСКИХ ПРОДУКТОВ, МЕХАНИЗМОВ И ИНФОРМАЦИИ

23. Чувствительная природа криптографических продуктов, механизмов и информации, используемой для защиты конфиденциальности, целостности и доступности классифицированной информации НАТО, требует применения особых мер предосторожности помимо тех, которые необходимы для защиты другой классифицированной информации НАТО.

24. Защита криптографических продуктов, механизмов и информации должна соответствовать ущербу в случае провала защиты. Необходим реальный способ оценки и проверки защиты и правильного функционирования криптографических продуктов и механизмов, а также защиты и контроля криптографической информации.

25. В знак признания особой чувствительности криптографической информации необходимы специальные правила и органы в пределах НАТО и каждого государства-члена для управления получением, контролем и распространением криптографической информации НАТО для специально утвержденных лиц.

26. Также необходимо следовать специальным процедурам, которые регулируют обмен технической информацией, а также отбор, производство и закупку криптографических продуктов и механизмов.

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРЕДАЧИ ДАННЫХ

27. Меры безопасности должны реализовываться для защиты от компрометации информации под грифом "НАТО - Конфиденциально" и выше посредством неумышленных электромагнитных излучений. Меры должны соответствовать риску использования и чувствительности информации.

ОСОБЫЕ ОБЯЗАННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Руководство НАТО по консультациям, командованию и управлению

28. В качестве главного комитета по политической стратегии руководство НАТО по консультациям, командованию и управлению (*C3*) поддерживает военный комитет НАТО и политические власти НАТО в процессе ратификации потенциала *C3* и проектов путем проверки оперативных требований *C3*. Руководство НАТО по консультациям, командованию и управлению отвечает за обеспечение безопасных и совместимых в НАТО систем *C3*.

Национальный орган безопасности связи (NCSA)

29. Каждое государство НАТО должно определить *NCSA*. Основные задачи *NCSA* следующие:

(a) контроль криптографической технической информации, связанной с защитой информации НАТО в пределах их стран;

(b) гарантия того, что криптографические системы, продукты и механизмы по защите информации НАТО эффективно и рационально отобраны, оперируются и обслуживаются; и

(c) поддержка связи по вопросам безопасности связи НАТО и связанным с ней техническим вопросам информационной безопасности, как гражданским, так и военным, с соответствующими национальными органами и органами НАТО.

Национальный орган распространения (NDA)

30. Каждая страна должна определить НОР, который отвечает за управление криптосредствами НАТО в пределах своих стран, а также обеспечить, что соответствующие процедуры и каналы, установленные для всестороннего учета, защищают обработку, хранение и распространение всех криптосредств.

ПРИЛОЖЕНИЕ "G"
МЕРЫ ПРОТИВ УТЕЧКИ ГОСУДАРСТВЕННОЙ СЕКРЕТНОЙ

ИНФОРМАЦИИ,
НАХОДЯЩЕЙСЯ В РАСПОРЯЖЕНИИ ПРОМЫШЛЕННОСТИ

ВВЕДЕНИЕ

1. Настоящее Приложение рассматривает аспекты безопасности промышленных операций, которые исключительны для переговоров и заключения секретных контрактов НАТО и их исполнением в промышленности, включая раскрытие классифицированной информации НАТО во время переговоров перед заключением контракта. Настоящее Приложение формулирует политику безопасности для:

(a) переговоров и заключения секретных контрактов НАТО;
(b) требований безопасности к секретным контрактам НАТО;
(c) раскрытия секретной информации НАТО при заключении контракта;
(d) допуска к секретной информации для контрактов НАТО;
(e) международных перевозок секретного материала НАТО;
(f) международных визитов; и
(g) временного персонала в рамках проекта/программы НАТО.

2. Настоящее Приложение сопровождается инструкцией промышленной безопасности, которая содержит подробные требования и процедуры. Инструкция включает в себя требования по переговорам и заключению секретных контрактов НАТО, требования безопасности для секретных контрактов НАТО, национальные органы по предоставлению допуска к секретной информации на объекте и для персонала, органы международных перевозок и визитов, список различных организаций, вовлеченных в секретные контракты НАТО, и их обязанности, а также список программ/проектов НАТО, участвующих стран и агентств НАТО.

ПЕРЕГОВОРЫ И ЗАКЛЮЧЕНИЕ СЕКРЕТНЫХ КОНТРАКТОВ НАТО

3. Основной контракт программы/проекта НАТО должен быть согласован и заключен программой/проектным агентством/офисом НАТО (*NPA/NPO*). Для всех подрядчиков, работающих по контракту, требуется допуск к секретной информации под грифом "НАТО - конфиденциально" и выше. Для контрактов под грифом "НАТО - для ограниченного пользования" допуск не требуется, если неоговорено иное национальными правилами и положениями безопасности.

4. *NPA/NPO*, заключающие контракт, должны гарантировать, что представители подрядчика, участвующие в переговорах по контракту под грифом "НАТО - конфиденциально" и выше, имеют соответствующую категорию допуска и получат доступ только к классифицированной информации НАТО, необходимой для заключения контракта.

5. После того, как основной договор был заключен, основной подрядчик может заключать субподряд с другими подрядчиками, т.е. субподрядчиками. Субподрядчики могут также заключать субподряды с другими субподрядчиками. Если потенциальный субподрядчик расположен и работает в государстве, не являющемся членом НАТО, разрешение на заключение субподряда должно быть получено от *NPA/NPO* (см. Приложение Е, параграфы 29-33). Если NPA/NPO установило ограничения на заключение контракта для государств НАТО, которые не участвуют в программе/проекте, то *NPA/NPO* должны выдать разрешение до обсуждения контракта с подрядчиками из данных стран.

6. По заключению основного контракта *NPA/NPO* должны уведомить Органы национальной безопасности/обозначенные органы безопасности (*NSA/DSA*) основного подрядчика и гарантировать, что письмо по аспекту безопасности и/или инструкция по безопасности проекта предоставлены основному подрядчику вместе с контрактом (см. параграфы 8 и 9 ниже).

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ДЛЯ СЕКРЕТНЫХ КОНТРАКТОВ НАТО

7. Головной подрядчик и субподрядчики должны быть обязаны по контакту под угрозой его расторжения принимать все меры, предписанные *NSA/DSA* для защиты и сохранности всей классифицированной информации НАТО, вверенной подрядчику, либо включенной в статьи, разработанные подрядчиком.

8. Секретные контракты НАТО для главных программ/проектов должны содержать инструкции по безопасности программы в качестве приложения; частью инструкции по безопасности программы должно быть "Руководство по классификации безопасности проекта". Все другие секретные контракты НАТО должны включать, как минимум, письмо по аспекту безопасности, которое может являться инструкцией по безопасности программы, сокращенной в масштабе. В последнем случае Руководство по классификации безопасности проекта можно упоминать как "Перечень классификации безопасности".

Инструкции по безопасности программы и/или письмо по аспекту безопасности, в зависимости от масштаба программы/проекта, должны быть единственным документом-источником для программы/проекта и использоваться в целях стандартизации процедур безопасности программы/проекта среди участвующих стран и органов НАТО и их подрядчиков.

9. Ответственность за применение классификации безопасности в элементах программы/проекта, имеющих отношение к продукту, в котором все элементы точно определены и их классификация предопределена, лежит на *NPA/NPO* по контракту, действующему в сотрудничестве с *NSA/DSA* участвующих государств-членов НАТО.

10. Классификация элементов информации программы/проекта, связанных с

возможными субподрядами, основывается на Руководстве по классификации безопасности проекта/программы.

РАСКРЫТИЕ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИИ НАТО В КОНТРАКТАХ

11. Раскрытие классифицированной информации НАТО должно производиться с согласия источника и в соответствии с другими применимыми приложениями к политике безопасности НАТО и поддерживающей инструкции по промышленной безопасности.

ДОПУСК К ПРОМЫШЛЕННОЙ СЕКРЕТНОЙ ИНФОРМАЦИИ ДЛЯ КОНТРАКТОВ НАТО

Общая часть

12. Политика, описанная в последующих параграфах для объектов и индивидов, применяется в контрактах и субподрядах.

Допуск к секретной информации на объекте

13. *NSA/DSA* (органы национальной безопасности/обозначенные органы безопасности) каждого государства-члена НАТО отвечает за гарантию того, что любой объект, расположенный и являющийся частью данной страны, которая потребует допуска к информации под грифом "НАТО - конфиденциально" и выше для вступления в предконтрактные переговоры или подачи заявки на секретный контракт НАТО, предпринял защитные меры безопасности, необходимые для получения права на допуск к секретной информации на объекте. Более того, работники объекта, которым требуется доступ к секретной информации НАТО, должны пройти соответствующую проверку и быть проинструктированы перед предоставлением сертификата о допуске к классифицированной информации. Допуск должен основываться на уровне классификации информации, ее объеме и характере и количестве индивидов, которым потребуется доступ к ней в ходе подготовки заявок или переговоров.

14. Подрядчик может принимать участие в предконтрактных переговорах, подавать заявки или выполнять секретный контракт НАТО при условии, что *NSA/DSA* государства, в котором расположен и работает подрядчик, присвоило объекту подрядчика требуемый уровень допуска к секретной информации на объекте.

15. Оценка, проводимая перед присвоением категории допуска, должна соответствовать требованиям и критериям, изложенным в поддерживающей инструкции промышленной безопасности.

16. Недостаток допуска к секретной информации для работников объекта не должен препятствовать подрядчику в подаче заявки на контракт или субподряд под грифом " НАТО - для ограниченного пользования". Страна, которая на основании своих национальных правил и положений по безопасности требует допуска к секретной информации для контракта или субподряда под грифом "НАТО - для ограниченного пользования", не должна дискриминировать подрядчика из страны, не требующей допуска, но должна гарантировать, что подрядчик был уведомлен о своих обязанностях в отношении защиты информации и признает данные обязательства.

Допуск к секретной информации для работников объекта

17. Допуск к секретной информации должен предоставляться в соответствии с Приложением С (Безопасность персонала), политикой безопасности НАТО и поддерживающими инструкциями по безопасности персонала и промышленной безопасности.

18. Заявки на проведение проверки работников объектов подрядчика для допуска к секретной информации должны предоставляться в NSA/DSA, которые отвечают за объект. При подаче заявки для проверки или инициации допуска к секретной информации объект должен включать следующее:

(a) подлинность и классификацию безопасности контракта или субподряда НАТО, и

(b) уровень секретной информации НАТО, к которой будет иметь доступ работник.

19. Если объект желает нанять гражданина государства, не являющегося членом НАТО, на должность, которая требует доступа к секретной информации НАТО, обязанностью NSA/DSA страны, в которой расположен и работает нанимающий объект , является выполнить процедуры по присвоению категории допуска, предписанные здесь, и определить, что индивиду можно предоставить допуск в соответствии с требованиями Приложения С и поддерживающими инструкциями по безопасности персонала и промышленной безопасности.

МЕЖДУНАРОДНЫЕ ПЕРЕВОЗКИ СЕКРЕТНОГО МАТЕРИАЛА НАТО

Принципы безопасности, применимые ко всем формам перевозок

20. Необходимо применить следующие принципы при проверке предлагаемых мероприятий по безопасности для международных перевозок партий секретного материала:

(a) безопасность должна гарантироваться на всех этапах перевозок и при всех обстоятельствах от пункта отправки до окончательного пункта назначения;

(b) степень защиты партии должна определяться наивысшим уровнем классификации материала, содержащегося в ней;

(c) допуск к секретной информации должен быть получен по обстоятельствам, для компаний, обеспечивающих перевозки. В таких случаях персонал, привлеченный к перевозке партии, должен быть подвергнут проверке в соответствии с условиями настоящего Приложения:

(d) перевозки должны осуществляться, насколько это возможно, от пункта до пункта, и должны заканчиваться в кратчайшие сроки, насколько это позволяют обстоятельства; и

e) надзор необходимо осуществлять только при организации перевозок через территорию государств НАТО. Перевозки через территории государств, не являющихся членами НАТО, должны осуществляться при получении разрешения от *NSA/DSA* (органы национальной безопасности/обозначенные органы безопасности) страны грузоотправителя и в соответствии с поддерживающей инструкцией по информационной безопасности.

21. Мероприятия, связанные с партиями секретного материала, должны быть оговорены для каждой программы/проекта. Однако, такие мероприятия должны гарантировать, что не существует вероятности несанкционированного доступа к секретным материалам.

22. Стандарты безопасности для международных перевозок секретного материала НАТО перечислены в поддерживающей инструкции по информационной безопасности. Подробные требования по перевозу секретного материала НАТО в ручной клади, транспортировке секретного материала коммерческими авиалиниями в качестве груза, обеспечению охраны и сопровождения, и транспортировке взрывоопасных веществ, метательных взрывчатых веществ и других опасных субстанций, изложены в поддерживающей инструкции по промышленной безопасности.

МЕЖДУНАРОДНЫЕ ВИЗИТЫ

Общая часть

23. Мероприятия, описанные в данном разделе, относятся к международным визитам военных и гражданских представителей государств НАТО, гражданских и военных органов НАТО, и подрядчиков и субподрядчиков НАТО, которым необходимо посетить следующие точки по одобренной деятельности НАТО:

(a) правительственный департамент или учреждение другого государства-члена НАТО;

(b) объект подрядчика или субподрядчика другого государства-члена НАТО; или

(c) гражданский или военный орган НАТО.

24. Визиты, упомянутые в параграфе 23(a) и (b) выше, должны быть одобрены NSA/DSA государства НАТО, в котором будет проводиться визит(-ы), принимая во внимание следующее:

(a) у визита есть официальная цель, относящаяся к программе или проекту НАТО; и

(b) все посетители имеют соответствующую категорию допуска и служебную необходимость в информации, связанной с проектом или программой НАТО или деятельностью НАТО.

25. Правительственные департаменты и учреждения, подрядчики и субподрядчики и гражданские и военные органы НАТО, принимающие посетителей, должны гарантировать, что:

(a) визиты соответствуют требованиям, изложенным в параграфе 24 выше;

(b) посетителям предоставлен доступ только к секретной информации НАТО, относящейся к цели данного визита; и

(c) сохраняются данные обо всех посетителях, включая их имена, организации, которые они представляют, дату(-ы) визита(-ов) и имя (имена) приезжавших лиц. Такие данные должны сохраняться в соответствии с национальными требованиями.

26. Правительственные департаменты и учреждения, подрядчики и субподрядчики, намеревающиеся послать персонал в международный визит, должны предоставить в *NSA/DSA* посещаемого объекта через свои *NSA/DSA* либо согласованные официальные каналы заявку на проведение международного визита в соответствии с процедурами, изложенными в инструкции по промышленной безопасности. Заявка на проведение международного визита должна гарантировать то, что каждый посетитель имеет действительную соответствующую категорию допуска.

27. Если это разрешено национальными правилами и положениями безопасности, визиты под грифом "НАТО - для ограниченного пользования" и "НАТО - несекретно" могут организовываться напрямую между Офисом безопасности для посетителя и Офисом безопасности посещаемого объекта.

ВРЕМЕННЫЙ ПЕРСОНАЛ В РАМКАХ ПРОЕКТА/ПРОГРАММЫ НАТО

28. Когда индивид, получивший право на доступ к секретной информации НАТО, временно переводится из одного объекта на другой в рамках одной и той же программы/проекта НАТО, но в другое государство-член НАТО, исходный объект индивида должен подать заявку в свои *NSA/DSA* о предоставлении Сертификата о присвоении категории допуска для индивида в *NSA/DSA* объект, куда он временно направляется. Временный работник должен быть назначен на должность в

соответствии с процедурами по подаче заявок на проведение международного визита, которые изложены в инструкции по промышленной безопасности, и в соответствии с национальными правилами и положениями безопасности.

СЛОВАРЬ

Подотчетная информация	Вся информация под грифом "Совершенно Секретно" (*CTS*) и "НАТО - Секретно" (NS) и вся информация особой категории (такая как ATOMAL).
Доступность	Свойство информации и материала быть доступными и используемыми по требованию лиц или организаций, имеющих на это санкцию.
Нарушение безопасности	Преднамеренное или случайное действие или бездействие, противоречащее политике безопасности НАТО и поддерживающим директивам, которое приводит к свершившейся или возможной компрометации классифицированной информации НАТО или поддерживающих услуг и ресурсов (включая, например, секретную информацию, утерянную во время перевозки; оставленную в неохраняемой зоне, где несанкционированные лица могут иметь несанкционированный доступ; невозможность найти подотчетный документ; секретная информация подверглась несанкционированным изменениям; была уничтожена несанкционированным способом или для коммуникационных информационных систем поступил отказ от обслуживания).
Секретная информация	Любая информация (а именно, сведения, которые можно передавать в любой форме) или материал, требующие защиты от несанкционированного разглашения, и которые были охарактеризованы таковыми по классификации безопасности.
Компетентный орган	Орган, определенный Национальным органом безопасности государства НАТО (*NSA*), который уполномочен проводить процедуры по присвоению своим гражданам категории допуска к классифицированной информации НАТО.
Компрометация	Компрометацией обозначается ситуация, при которой вследствие нарушения безопасности или враждебных действий (таких как шпионаж, акты терроризма, диверсия или кража) классифицированная информация НАТО утратила свою конфиденциальность, целостность или доступность, или поддерживающие услуги и ресурсы утратили свою целостность или доступность. Это включает в себя утерю, разглашение несанкционированным лицам (например, посредством шпионажа или СМИ), несанкционированное видоизменение, уничтожение несанкционированным способом, либо отказ от обслуживания.
Конфи-денциальность	Свойство информации не быть доступной или раскрытой несанкционированными лицами или организациями.

Допуск к секретной информации на объекте (FSC)	Административное определение NSA/DSA, гласящее с точки зрения безопасности, что объект может предоставить защиту безопасности классифицированной информации НАТО особой классификации или ниже, и что персонал, которому требуется доступ к классифицированной информации НАТО, был соответствующим образом проверен и проинструктирован в отношении требований безопасности НАТО, необходимых для выполнения секретных договоров НАТО.
Охранники	Гражданский (работники правительства или участвующего подрядчика) или военный персонал, который может быть вооружен или безоружен. Они могут выполнять только обязанности по охране или совмещать эти обязанности с другими.
Страна пребывания	Общий термин: страна, в которой расположен военный или гражданский орган НАТО Промышленная безопасность: страна, избранная официальным органом НАТО выступать в качестве правительственного агентства и принимающая обязательства выполнять основной контракт НАТО. Страны, в которых выполняются субподряды, не именуют странами пребывания.
Информация	Сведения, передаваемые в различных формах.
Информационная безопасность (INFOSEC)	Применение мер безопасности по защите имеющейся информации, хранящейся или передаваемой через средства связи, системы информационного обслуживания и другие электронные системы, против утраты конфиденциальности, целостности или доступности, как случайной, так и преднамеренной, и для предотвращения утраты целостности или доступности самих систем. Примечания. 1. Меры информационной безопасности включают компьютерную безопасность, обеспечение скрытности связи, конфиденциальность передачи данных, криптографическую защиту. 2. Такие меры также включают обнаружение, документирование и противодействие угрозе информации и системам.
Нарушение	Нарушение безопасности - это действие или бездействие, преднамеренное или случайное, противоречащее политике безопасности НАТО и поддерживающим директивам, которое не приводит к свершившейся или возможной компрометации секретной информации НАТО (например, секретная информация, оставленная неохраняемой на охраняемом объекте, где все лица имеют соответствующую категорию допуска; секретная информация была оставлена в открытом виде и т.д.).
Целостность	Свойство, обозначающее что информация (включая такие данные, как зашифрованный текст) не была изменена или уничтожена несанкционированным способом.
	Визиты лиц, подчиненных одному *NSA/DSA* (национальному органу безопасности государства НАТО/назначенному органу безопасности) или принадлежащих органу НАТО, на

Международные визиты	объект или органы, контролируемые другим *NSA/DSA* или НАТО, которые потребуют или станут причиной доступа к классифицированной информации, или где, в независимости от уровня секретности, посещение при поддержке НАТО учреждения или органа, находящихся под национальной юрисдикцией, требует одобрения соответствующим *NSA/DSA*. Все гражданские и военные органы НАТО подпадают под юрисдикцию безопасности НАТО.
Жизненный цикл	Жизненный цикл информации заключает в себе этапы планирования, сбора, создания или формирования информации; ее организацию, восстановление, использование, доступность и передачу; ее хранение и защиту; и, наконец, ее размещение через сдачу в архив или уничтожение.
Главная программа/ проект	Программа или проект большого значения, обычно с привлечением более двух стран и мер безопасности, которые превышают обычные основные требования, описанные в политике безопасности НАТО.
Материал	Материал включает в себя документы, а также любые элементы механизмов, оборудования/компонентов, оружия или инструментов, произведенных, или находящихся в процессе производства.
Граждане	Граждане включают в себя "подданных Королевства", "граждан Штатов" и "осевшие иммигранты в Канаде". "Осевшие иммигранты в Канаде" - это лица, которые прошли национальную проверку, включая проверку местожительства, сведений о судимости и проверку безопасности, и которые собираются получить законное разрешение на постоянное местожительстве в стране.
Национальный орган безопасности (*NSA*)	Орган государства-члена НАТО, который несет ответственность за поддержание безопасности классифицированной информации НАТО в национальных агентствах и элементах, военных или гражданских, в пределах своей страны и за ее пределами.
НАТО	НАТО обозначает Организацию Североатлантического договора и органы, действующие на основании Соглашения о статусе Организации Североатлантического договора, национальных представителей и международного штаба, подписанного 20 сентября 1951 года в Оттаве, или Протоколом о статусе Международных военных штабов, созданных в соответствии с Североатлантическим договором, подписанным в Париже 28 августа 1952 года.
Секретный контракт/ договор НАТО	Любой контракт/договор, разработанный гражданским/ военным органом НАТО либо государством-членом НАТО в поддержку финансируемой или управляемой программы/проекта НАТО, которая потребует доступа или выдачи секретной информации НАТО.
	(a) информация - сведения, которые можно передавать в любой форме; (b) классифицированной информацией является информация или материал, требующие защиты от несанкционированного разглашения, и которые были

Классифицированная информация НАТО	охарактеризованы таковыми по классификации безопасности; (c) понятие "материал" включает в себя документы, а также любые элементы механизмов, оборудования/компонентов, вооружения либо произведенных, либо находящихся в процессе производства; (d) понятие "документ" означает любую записанную информацию в независимости от ее физической формы или характеристик, включая, без ограничений, письменную и печатную продукцию, карточки и записи обработанных данных, карты, чертежи, фотографии, изображения, рисунки, гравюры, наброски, рабочие записи и бумаги, машинописные копии или копировальные ленты, или копирование любым способом или процессом, а также звуковые, голосовые, магнитные, электронные, оптические или видео записи в любой форме, и портативное оборудование для автоматической обработки данных со стационарных или съемных компьютерных носителей данных.
Военный комитет НАТО (NAMILCOM)	Наивысший военный орган НАТО; военный комитет отвечает за общее ведение военных дел. Военный комитет несет ответственность за одобрение и предоставление приоритетности, с оперативной точки зрения, исполнительских требований предъявляемых к стратегическим командованиям.
Проверка благонадежности личного состава (персонала) для допуска к секретной информации НАТО(PSC)	Определение, согласно которому индивид подходит для получения доступа к классифицированной информации НАТО.
Организация НАТО по производству и тыловому обеспечению (NPLO)	Вспомогательный орган, учрежденный в рамках НАТО для реализации задач вытекающих из договора, которому Североатлантический совет предоставляет четко определенную организационную, административную и финансовую независимость. Он должен состоять из совета директоров, и исполнительного органа, состоящего в свою очередь из генерального менеджера и персонала.
Программа НАТО	Одобренная Советом программа, которая контролируется управлением/офисом НАТО в соответствии с положениями НАТО.
Проект НАТО	Одобренная Советом проект, которая контролируется управлением/офисом НАТО в соответствии с положениями НАТО.
Агентство по управлению	

проектами НАТО	Исполнительный орган Организации НАТО по производству и тыловому обеспечению.
Служебная необходимость	См. "Принцип служебной необходимости" ниже
Переговоры	Термин охватывает все аспекты заключения контрактов или субподрядов от первоначального "уведомления о намерении подавать заявку на участие" до окончательного решения о заключении контракта или субподряда.
Зона открытого хранения	Зона, созданная в соответствии с требованиями безопасности и используемая с разрешения главы гражданского или военного органа для открытого хранения секретной информации.
Источник	Страна или международная организация, под чьим руководством информация была создана или внедрена в НАТО.
Страна гражданства	Королевство, подданным которого является индивид или государство гражданином которого является индивид.
Национальный орган безопасности (NSA)	Национальный орган безопасности Королевства или государства, подданным или гражданином которого является индивид.
Проверка благо-надежности личного состава (персонала) для допуска к секретной работе	Определение, согласно которому индивид подходит для получения доступа к классифицированной информации.
Главный контракт	Первоначальный контракт, возглавляемый офисом по управлению проектов НАТО/Агентством/Офисом для программы/проекта.
Главный подрядчик	Промышленная, коммерческая или другая организация государства-члена, которая заключила контракт с агентством/офисом по управлению проектом НАТО для предоставления услуг или производства продукции в рамках проекта НАТО, и который в свою очередь может заключить согласованный субдоговор с потенциальными субподрядчиками.
Принцип служебной необходимости	Принцип, согласно которому было позитивно установлено, что предполагаемому реципиенту требуется доступ, знание и владение информацией для выполнения официальных задач и обязанностей.
Руководство по классифи-кации безо-	Часть инструкций по безопасности программы (проекта), которая определяет элементы программы, являющиеся секретными с обозначением уровней классификации безопасности. Руководство по классификации безопасности может увеличиваться в объеме в течение жизненного цикла программы, а элементы информации

пасности программы/ проекта	могут быть рассекречены или отнесены к более низкой категории секретности.
Инструкция по безопасности программы/ проекта (*PSI*)	Комплекс положений/процедур по безопасности, основанных на политике безопасности НАТО и поддерживающих директивах, которые применяются в особых проектах/программах в целях стандартизации процедур безопасности. Инструкции также составляют Приложение к основному контракту и могут быть изменены в течение жизненного цикла программы. Для субдоговоров, заключаемых в рамках программы, инструкции по безопасности программы составляют основу письма по аспекту безопасности.
Риск	Вероятность уязвимости, успешно используемая угрозой, ведущая к компрометации конфиденциальности, целостности и/или доступности и продолжительному ущербу.
Управление риском	Систематичный подход к определению контрмер по безопасности, необходимых для защиты информации и поддерживающих служб и ресурсов, основанный на оценке угроз и уязвимых мест. Управление риском затрагивает планирование, организацию, направление и контроль ресурсов для обеспечения того, что риск остается в приемлемых пределах.
Письмо по аспекту-безопасности (SAL)	Документ, выдаваемый соответствующим органом как часть любого секретного договора или субдоговора, отличного от главной программы/проекта и определяющего требования безопасности или возникающие из него элементы, требующие обеспечения безопасности.
Гарантия безопасности	Гарантия, предоставляемая НАТО напрямую или через государство НАТО либо гражданский/военный орган НАТО.
Перечень классификаций по безопасности	Часть письма по аспекту безопасности, которая описывает секретные элементы контракта, с обозначением грифов секретности. В случае, когда договоры заключаются в рамках программы/проекта, такие элементы информации извлекаются из инструкций по безопасности программы/проекта, выпущенных для данной программы.
Информация особой категории	Такая информация, как сведения о ядерном оружии (*ATOMAL*) или Единый комплексный оперативный план (*SIOP*), к которому применяются дополнительные процедуры обработки/защиты.
Субдоговор/ субподряд	Договор, заключаемый главным подрядчиком с другим подрядчиком (т.е. субподрядчиком) для предоставления товаров или услуг.
Субподрядчик	Подрядчик, с которым основной подрядчик заключает субдоговор.
Угроза	Вероятность компрометации, утери или кражи секретной информации НАТО или поддерживающих служб и ресурсов. Угроза может определяться ее источником, мотивом или результатом, она может быть преднамеренной или случайной, явной или скрытной, внешней или внутренней.

Уязвимость	Недостаток, атрибут или нехватка контроля, которые способствуют приведению угрозы в действие против секретной информации НАТО или поддерживающих услуг и ресурсов.

Текст переведен на русский язык в соответствии с оригиналом.

Начальник Главного управления международных программ

Вооруженных Сил Республики Казахстан

полковник *В. Райхель*

НАТО НЕСЕКРЕТНО

17 июня 2002 года **ДОКУМЕНТ**

C-M(2002)50

МЕРЫ ЗАЩИТЫ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ НАТО РАЗВЕРНУТЫХ СИЛ И ОБЪЕКТОВ (СРЕДСТВ) НАТО ПРОТИВ УГРОЗЫ ТЕРРОРИЗМА Примечание Генерального секретаря

1. Данный документ является результатом поставленной задачи Совета по развитию директив для "Развернутых сил и объектов НАТО против угрозы терроризма". Проект документа был составлен группой Экспертов под эгидой комитета по вопросам безопасности НАТО (NSC), состоящего из соответствующих национальных специалистов и военных представителей. Он также включает в себя исправленную версию одной из частей "Защиты безопасности командований и агентств НАТО", Приложение *E* к *C-M*(55)15 (окончательному). Он был одобрен Советом по процедуре умолчания 26 марта 2002 года (C-M(2002)22-REV1 и перечень его мероприятий).

2. Настоящий документ аннулирует все предыдущие версии Приложения "E" к C-M (55)15(окончательному), которые должны быть уничтожены.

3. Копия настоящего документа будет включена в компендиум, содержащий 2 документа по политике безопасности и вспомогательные директивы, которые будут разосланы всем текущим держателям C-M(55)15(окончательного) в ближайшем будущем.

(подписано) Джордж Робертсон

Приложения: 3 Оригинал: Английский

МЕРЫ ЗАЩИТЫ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ НАТО РАЗВЕРНУТЫХ СИЛ И ОБЪЕКТОВ (СРЕДСТВ) НАТО ПРОТИВ УГРОЗЫ ТЕРРОРИЗМА

1. ВВЕДЕНИЕ

1.1 Настоящий документ С-М закладывает политику по мерам контртерроризма и против диверсии для:

- ЧАСТЬ 1: гражданские и военные органы и силы НАТО в пределах территории государств-членов НАТО. Данные меры должны соответствовать законодательству страны пребывания, в которой расположены гражданские или военные органы НАТО или развернуты силы НАТО.

- ЧАСТЬ 2: силы и объекты (средства) НАТО, развернутые за пределами территории государств-членов (операции вне 5 статьи). Данные меры применяются в местах размещения персонала и объектов (средств) НАТО с ограниченной или отсутствующей поддержкой страны пребывания, на которые можно рассчитывать для обеспечения адекватного реагирования на угрозы терроризма или диверсии.

1.2 Данный документ С-М образует часть политики безопасности НАТО.

2. ЧАСТЬ 1: МЕРЫ ЗАЩИТЫ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ НАТО, РАЗВЕРНУТЫХ СИЛ И ОБЪЕКТОВ (СРЕДСТВ) НАТО ПРОТИВ УГРОЗЫ ТЕРРОРИЗМА В ПРЕДЕЛАХ ТЕРРИТОРИИ ГОСУДАРСТВ-ЧЛЕНОВ НАТО

2.1 УГРОЗЫ И РИСКИ

2.1.1 Риски для гражданских и военных органов НАТО, возникающие из угрозы терроризма, могут быть 6 типов:

(a) общая безопасность персонала;

(b) отказ в поставке необходимых ресурсов и услуг, который воспрепятствует или снизит возможность выполнения задачи;

(c) физический ущерб;

(d) нарушение выполнения задачи;

(c) нарушение свободы передвижения, либо

(d) нарушение общей безопасности и стабильности в пределах территории государств-членов НАТО.

2.1.2 Потенциальная угроза гражданским и военным органам и лицам НАТО от террористической деятельности может исходить от:

(i) террористических организаций (которые могут включать в себя группы и индивидов), которые могут выбрать НАТО в качестве цели;

(ii) подрывной деятельности, причиняющей ущерб имуществу, ограничивающей способности индивидов и/или являющейся причиной утери необходимых ресурсов и услуг;

(iii) организованной преступности;

(iv) общественных беспорядков.

Виды угроз

2.1.3 Угроза насилия гражданским и военным органам НАТО может включать в себя:

(a) бомбовые атаки или атаки стрелкового орудия, взрыв машин, бомбы в ручной клади, "почтовые" бомбы и взрывчатые зажигательные устройства,

(b) убийство, похищение, захват заложников или запугивание персонала НАТО и их семей,

(c) демонстрации, которые могут быть организованы с целью насилия, могут привести к насилию/ущербу через конфронтацию,

(d) прямые атаки и незаконное занятие помещений или собственности НАТО как это случалось с посольствами и международными миссиями,

(e) ложные тревоги, а именно предупреждение, о якобы заложенной бомбе с намерением досадить,

(f) операции против необходимых/жизненноважных систем информационных технологий, включая посягательства на целостность и/или доступность этих систем,

(g) обезвреживание силой оружия, вооружения и оборудования, необходимого для достижения задачи, и

(h) оружие массового поражения (ОМП), а именно, химические и биологические атаки.

2.2 ОБЯЗАННОСТИ

Страны пребывания

2.2.1 Страны пребывания отвечают за обеспечение внешней защиты гражданским и военным органам НАТО. Страна пребывания решает, оказывается ли эта защита государственными контрразведывательными службами, правоохранительными органами или государственными оборонительными силами. По требованию, страна пребывания должна указать главе гражданского или военного органа НАТО то ведомство, с которым должны координироваться защитные планы по безопасности и на каком уровне. Страна пребывания также отвечает за информирование глав гражданских и военных органов НАТО об оценке угроз, исходящих от враждебных разведывательных служб, подрывных организаций, террористических групп и подобных элементов, когда того потребуют обстоятельства.

(a) Страна пребывания должна гарантировать, если не оговорено иное, что информация относительно угроз, имеющих отношение к гражданским и военным органам НАТО и их персоналу, находящемуся вне соответствующих территорий, передается через двусторонние каналы из страны в страну;

(b) страна пребывания должна предоставить рекомендации гражданским и военным органам НАТО относительно особых дополнительных контртеррористических мер для различных уровней угроз;

(c) страна пребывания несет ответственность за обеспечение таким персоналом и

оборудованием по безопасности для защиты персонала НАТО от угрозы терроризма за пределами помещений гражданских и военных органов НАТО в соответствии с государственными защитными стандартами и процедурами по безопасности страны пребывания. Обозначение персонала, находящегося под угрозой терроризма, а также меры безопасности, используемые для их защиты, определяются ведомством по безопасности страны пребывания с принятием во внимание предложений со стороны заинтересованных гражданских и военных органов НАТО (помимо других). Данные предложения должны быть обоснованы;

(d) для каждого гражданского и военного органа НАТО на своей территории страна пребывания должна определить канал контакта для передачи информации относительно угроз и координации внутренних планов по безопасности.

Направляющие страны

2.2.2 Направляющие страны должны обеспечить следующее:

(a) При выборе мест проживания для их персонала должен учитываться анализ безопасности, на основании опыта ведомств по безопасности страны пребывания. Затраты, которые несет принимающая страна на улучшение физической безопасности, должны ограничиваться местами проживания, официально финансируемыми ими;

(b) Развертывание персонала по безопасности и обеспечение защитного оборудования по безопасности направляющей страной для борьбы с какими-либо террористическими или подрывными угрозами координируется с ведомствами по безопасности страны пребывания и соответствующим гражданским или военным органом НАТО;

(c) информирование ведомства по безопасности страны пребывания и соответствующего гражданского или военного органа НАТО о какой-либо существующей угрозе какому-либо из их граждан в штабе НАТО или национальных делегациях, военных представительствах или миссиях связи, расположенных совместно с гражданским или военным органом НАТО.

Офис безопасности НАТО

2.2.3 Офис безопасности НАТО должен оказывать содействие в вопросах и процедурах контртерроризма и борьбы с подрывной деятельностью. Офис безопасности НАТО должен предоставить техническую оценку/обоснование соответствующему бюджетному комитету относительно строительных работ и оборудования/материалов контртеррористического и противодиверсионного назначения.

2.2.4 Офис безопасности НАТО должен провести проверку контртеррористических программ объекта/подразделения НАТО при проведении своих периодических поверок безопасности в пределах обязательного 18-месячного цикла проверок. Инспекционная группа Офиса безопасности НАТО будет осуществлять проверку и консультировать относительно адекватности контртеррористических разделов плана внутренней

безопасности объекта/подразделения и способности объекта/подразделения реализовывать данные контртеррористические разделы. Там где это уместно, инспекционная группа Офиса безопасности НАТО также проконсультирует относительно адекватности контртеррористической подготовки и программы учений объекта/подразделения, которые поддерживают план внутренней безопасности.

Гражданские и военные органы НАТО

2.2.5 Глава военного или гражданского органа НАТО должен определить, при необходимости проконсультировавшись с НАТО и государственными органами, ключевые учреждения и объекты под своей юрисдикцией, которые важны для продолжения функции, необходимой для выполнения основной задачи НАТО, принимая во внимание общие цели НАТО. Он также несет ответственность за планирование и реализацию следующих дополнительных контртеррористических и противодиверсионных мер по защите объектов, включая места проживания, обеспечиваемые НАТО, и персонала, размещенного в данных помещениях. Старший персонал НАТО должен быть представлен гражданскими или военными органами НАТО принимающей и направляющей стране. В целях достижения удовлетворительных и выгодных договоренностей в соответствии с подходом по управлению рисками, главы гражданских и военных органов НАТО обязуются:

(a) назначить своих контактных лиц для официальной связи с соответствующими органами безопасности страны пребывания через каналы, одобренные НАТО:

(i) получить общую оценку террористической угрозы;

(ii) провести мероприятия по получению и обмену информацией относительно особых угроз;

(iii) скоординировать контртеррористические меры, соизмеримые с оцениваемой угрозой; и

(iv) представить предложения как указано ниже в параграфе 2.3.1;

(b) поддерживать официальную связь старшего персонала НАТО или государственного персонала с органами безопасности страны пребывания через каналы, одобренные НАТО, для координации контртеррористических мер в случае существующей особой угрозы:

(i) персоналу, исходящей от террористических организаций, действующих в направляющих их странах; либо

(ii) гражданам определенной страны;

(c) установить систему оповещения, как описано ниже в параграфе 2.4.9, и определить обязанности по реализации заранее запланированных мер по управлению угрозой;

(d) установить процедуры, как указано ниже в параграфах 2.3.1 - 2.3.2, для

сообщения и донесения странам пребывания, направляющим странам, Офису безопасности НАТО к другим гражданским и военным органам НАТО относительно террористических угроз и происшествий.

2.3 ДОКЛАДЫ О ТЕРРОРИСТИЧЕСКОЙ ИЛИ ПОДРЫВНОЙ ДЕЯТЕЛЬНОСТИ

2.3.1 Доклады различных военных или гражданских органов о террористической/ подрывной деятельности или происшествиях должны отражать:

(a) орган, от которого исходит информация;

(b) характер и последствия угрозы или происшествия;

(c) предпринятые действия.

2.3.2 Во избежание дублирования докладов и в целях гарантированного обеспечения адекватной информацией заинтересованных органов власти, сведения о случаях угроз либо действительных террористических или подрывных инцидентах необходимо сообщать следующим образом:

(a) когда информация была получена от органов безопасности страны пребывания:

(i) военные органы НАТО должны доложить об особой угрозе или происшествии, органе, от которого исходит информация ("источник") и мерах, которые необходимо предпринять, следующему вышестоящему органу с копией в Офис безопасности НАТО ;

(ii) командиры национальных контингентов (включая страны, предоставляющие войска, но не являющиеся членами НАТО) должны докладывать в командные инстанции в своих столицах;

(iii) гражданские органы НАТО должны докладывать в соответствии с пунктом (i) выше напрямую в Офис безопасности НАТО;

(b) когда информация получена в рамках гражданского или Военного органа НАТО:

(i) военные органы НАТО должны докладывать об особой угрозе или происшествии и источнике вместе с мерами, которые необходимо предпринять, органам безопасности страны пребывания и, в соответствии с мероприятиями по параграфу 2.2.5 выше, в соответствующий вышестоящий или подчиненный штаб НАТО по вертикали управления с копией в Офис безопасности НАТО;

(ii) гражданские органы НАТО должны докладывать в соответствии с пунктом (i) выше в органы безопасности страны пребывания и в Офис безопасности НАТО.

2.4 ПЛАНИРОВАНИЕ БЕЗОПАСНОСТИ

Проектирование объектов НАТО

2.4.1 Проектирование объектов НАТО должно учитывать анализ безопасности; и включать в себя защиту материалов и резервное оборудование, необходимое для следующего:

(a) продолжения выполнения необходимых оперативных функций;

(b) защиты средств НАТО; и

(c) общей безопасности всего персонала.

План внутренней безопасности

2.4.2 Командиры объектов/подразделений НАТО должны подготовить план внутренней безопасности в целях обеспечения защиты безопасности объекта/ подразделения от террористических атак. План внутренней безопасности применяется для защиты персонала НАТО, членов их семей и других средств.

2.4.3 Целью плана внутренней безопасности является сокращение уязвимости путем сдерживания или обнаружения атаки или смягчения последствий террористической атаки или диверсионных актов. План безопасности должен быть разработан с использованием методологий, которая содержала бы следующие требования:

(a) определение средств объекта или учреждения;

(b) оценка последствий утери таких средств, влияющих на продолжение функции, необходимой для выполнения основной задачи НАТО;

(c) детальный анализ уязвимых мест объекта, который включает в себя оценку методов атаки, к которым они уязвимы.

2.4.4 На основании данных требований необходимо разработать свод мер безопасности, которые сократят уязвимость важных средств. Меры могут включать физические мероприятия (ограждения, ворота, двери, решетки), электронные меры (кабельное телевидение, внутренние или внешние сигнализации) или людские ресурсы (служба охраны и силы реагирования). План безопасности должен также определять возможности дополнительных мер или процедур безопасности (например, обыск посетителей), применение которых увеличивается при усилении бдительности и отменяется при снижении бдительности.

2.4.5 План безопасности должен разрабатываться в тесном взаимодействии с соответствующими органами страны пребывания в целях обеспечения полной защиты. Многие внутренние защитные меры зависят от силы или слабости дополнительных внешних мер, предпринимаемых страной пребывания. Лучшая защита в большей степени обеспечивается определенным количеством скоординированных и дополнительных мер, чем полной надеждой на один из видов защиты.

2.4.6 План внутренней безопасности должен включать:

(a) оценку террористической/подрывной угрозы;

(b) оценку управления рисками. Она должна включать, как минимум, оценку серьезности и уязвимости;

(c) меры безопасности, включая физическую безопасность;

(d) план реагирования на происшествие, который должен содержать:

(i) определение органа, ответственного за отдачу приказа на осуществление одной из стадий плана; и официальных лиц, несущих ответственность за реализацию особых мер, перечисленных в плане;

(ii) распределение обязанностей по командованию и управлению;

(iii) мероприятия на случай чрезвычайных ситуаций для сил поддержки и резервных

с и л ;

(iv) описание действий сил безопасности НАТО в и за пределами помещений НАТО в соответствии с законодательством страны пребывания;

(v) альтернативные средства связи для сил безопасности;

(vi) особые действия и обязанности, связанные с применением каждой из мер по усилению б д и т е л ь н о с т и ;

(e) План ликвидации последствий, включающий:

(i) Соответствующий персонал "первого реагирования", функцией которого является смягчить потерю/травматизм персонала и нанесение ущерба структурам/ средствам. Персонал быстрого реагирования включает в себя, но не ограничивается: медицинским персоналом, пожарными и спасательными группами, подразделениями по деконтаминации оружия массового поражения (ОМП) и персоналом безопасности.

(ii) Соответствующее планирование исследования места преступления правоохранительными органами, а также реагирования на потери персонала/ущерба собственности.

Персонал по безопасности

2.4.7 Гражданские и военные органы НАТО должны принять во внимание контртеррористический и противодиверсионный анализ при установлении или проверке мер по охране своих учреждений. Персонал по защите старших должностных лиц НАТО должен содержаться отдельно от других сил безопасности, а его развертывание должно координироваться с органами безопасности страны пребывания.

2.4.8 Гражданские и военные органы НАТО должны проводить подготовку своего персонала для выполнения своих функций в различных обстоятельствах путем официальных указаний и проведения учений с органами страны пребывания. Учения должны включать оповещение персонала в нерабочее время. В целях гарантийного обеспечения эффективной реализации плана безопасности в случае возникновения такой необходимости, чрезвычайно важно проводить подготовку задолго до прогнозируемой чрезвычайной ситуации.

Стандартная система оповещения

2.4.9 Стандартная система оповещения должна быть установлена во всех штабах гражданских и военных органов НАТО. Данная система оповещения должна состоять из четырех отдельных этапов, помимо стандартных, и содержать основные минимальные меры, применяемые во всех гражданских и военных органах НАТО. Подробные данные относительно системы оповещения и соответствующей системы связи и основных минимальных мерах для каждой стадии, а также другие необходимые или рекомендуемые меры будут разрабатываться под эгидой Комитета безопасности НАТО (см. Приложение 1 "Состояния системы оповещения НАТО" и Приложение 2 " Состояния системы оповещения НАТО - минимальные меры").

Составление бюджета для физической защиты и других защитных материалов

2.4.10

(a) Гражданские и военные органы НАТО должны подать заявку на выделение финансовых средств из военного или гражданского бюджета НАТО для обеспечения физической защиты их объектов (включая официальные резиденции НАТО). К бюджетным заявкам должна прилагаться оценка угроз, произведенная органами безопасности страны пребывания во взаимодействии с гражданским и военным органом НАТО;

(b) Заявки на выделение финансовых средств НАТО для обеспечения специальных систем связи, используемых за пределами объектов НАТО как часть контртеррористических или противодиверсионных мер, требуют обоснования, отражающего полное взаимодействие с органами безопасности страны пребывания;

(c) Выделение бронированных транспортных средств из бюджета НАТО должно ограничиваться Генеральным секретарем и Верховным главнокомандующим объединенными вооруженными силами НАТО в Европе. Для чрезвычайных ситуаций, когда существует доказанная угроза, для противостояния которой, по мнению органов безопасности страны пребывания, необходим бронированный автомобиль, и когда он не может обеспечиваться страной пребывания или направляющей страной, бронированное транспортное средство может быть арендовано из фондов НАТО в соответствии с процедурами, установленными заблаговременно соответствующими финансовыми комитетами, на весь период существования угрозы;

(d) Другое оборудование для личной защиты, такое как пуленепробиваемая одежда и специальное оружие, может быть получено из фондов НАТО в разумных количествах для использования персоналом безопасности НАТО. Обоснование для заявки на получение такого оборудования должно включать описание характера использования оборудования.

Фонды НАТО не должны использоваться для приобретения оборудования личной защиты для использования персоналом, не занимающим установленные НАТО должности, и только в исключительных случаях выделение средств может быть одобрено на приобретение такого оборудования для использования другим персоналом помимо персонала безопасности НАТО.

2.4.11 Контртеррористические и противодиверсионные мероприятия и деятельность, связанные с гражданскими и военными органами НАТО, должны контролироваться Офисом безопасности НАТО. В этой связи Офис безопасности НАТО должен получить копию общей оценки угроз, применимой для каждого штаба или группы штабов. Гражданские и военные органы НАТО должны направлять в Офис безопасности НАТО две копии своих контртеррористических планов. Офис безопасности НАТО необходимо информировать об особой деятельности посредством системы доклада, описанной в параграфах 2.3.1 - 2.3.2 выше.

2.4.12 Контртеррористические и противодиверсионные мероприятия, включая действие плана внутренней безопасности, должны изучаться во время программы проверки безопасности для гражданских и военных органов НАТО. Данные, полученные во время этих проверок, должны прилагаться к отчету о проверке.

3. ЧАСТЬ 2: МЕРЫ ЗАЩИТЫ ГРАЖДАНСКИХ И ВОЕННЫХ ОРГАНОВ НАТО, РАЗВЕРНУТЫХ СИЛ И ОБЪЕКТОВ (СРЕДСТВ) НАТО ПРОТИВ УГРОЗЫ ТЕРРОРИЗМА ЗА ПРЕДЕЛАМИ ТЕРРИТОРИИ ГОСУДАРСТВ-ЧЛЕНОВ НАТО

3.0 Настоящий Раздел устанавливает политику контртеррористических мер для сил и объектов (средств) НАТО, развертываемых за пределами территории государств-членов НАТО (операция вне 5 статьи). Данные меры применяются в зонах, где развертывается персонал и объекты (средства) НАТО, с недостаточной поддержкой , на которую можно полагаться для обеспечения адекватного реагирования на террористическую/подрывную угрозу.

3.1 ПРИМЕНЕНИЕ МЕР ПО КОНТРТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЕ ЗА ПРЕДЕЛАМИ ТЕРРИТОРИИ ГОСУДАРСТВ-ЧЛЕНОВ НАТО

3.1.1 Меры по контртеррористической защите, описанные в Части 2, применимы только к операциям НАТО, проводимым вне 5 статьи, и где структура страны пребывания, если таковая существует, выпадает из юрисдикции государства-члена НАТО.

3.1.2 Меры, изложенные в данном разделе, применяются когда возникает террористическая угроза, которая может подвергнуть опасности силы и объекты НАТО .

3.2 УГРОЗЫ И РИСКИ

3.2.1 Риски для гражданских и военных органов НАТО, возникающие из угрозы терроризма, могут быть 6 видов:

(a) общая безопасность персонала;

(b) отказ в поставке необходимых ресурсов и услуг, который воспрепятствует или снизит возможность выполнения задачи;

(c) физический ущерб;

(d) нарушение выполнения задачи;

(e) нарушение свободы передвижения, либо

(f) нарушение общей безопасности к стабильности за пределами территории государств-членов НАТО.

3.2.2 Угроза терроризма силам и объектам (средствам) НАТО, развертываемым за

пределами территории государств-членов НАТО, от организаций, групп и индивидов, которые могут избрать персонал и объекты (средства) НАТО в качестве цели для осуществления своих намерений, как в пределах, так и за пределами государств-членов НАТО, включает:

(a) бомбовые атаки или атаки стрелкового оружия, взрыв машин, бомбы в ручной клади, "почтовые" бомбы и взрывчатые зажигательные устройства,

(b) убийство, похищение, захват заложников или запугивание персонала НАТО и их семей,

(c) демонстрации, которые могут быть организованы с целью насилия, могут привести к насилию/ущербу через конфронтацию,

(d) прямые атаки и незаконное занятие помещений или собственности НАТО как это случалось с посольствами и международными миссиями,

(e) ложные тревоги, а именно предупреждение о якобы заложенной бомбе с намерением досадить,

(f) операции против необходимых/жизненноважных систем информационных технологий, включая посягательства на целостность и/или доступность этих систем,

(g) оружие массового поражения (ОМП), а именно, химические и биологические атаки,

(h) обезвреживание силой оружия, вооружения и оборудования, необходимого для достижения задачи.

Оценка угрозы

3.2.3 Потенциальная угроза террористической деятельности против сил НАТО и персонала, выполняющего операции НАТО за пределами территории государств-членов НАТО, подлежит оценке до принятия контрмер. Несмотря на то, что обстоятельства и условия зависят от операции, процесс оценки, как минимум, должен обеспечивать следующее:

(a) Источники информации об угрозе оцениваются на предмет надежности, насколько это возможно,

(b) Анализ информации об угрозе оправдывает применение контртеррористических мер,

(c) Оценка угрозы является своевременной и текущей, и

(d) Разрабатывается местная стратегия управления рисками.

3.3 ОБЯЗАННОСТИ

3.3.1 Общие

Распределение контртеррористических обязанностей и задач определяется 4 различными условиями, в которых силы НАТО могут действовать за пределами территории государств-членов НАТО:

(a) Толерантные, при полной поддержке со стороны страны пребывания;

(b) Полутолерантные, в которых органы страны пребывания, в общем оказывают

сотрудничество, однако без выделения достаточных средств или осуществления контроля для обеспечения эффективной поддержки;

(c) Нетерпимые, когда местные власти и население настроены враждебно или не оказывают поддержки;

(d) В международных водах и/или воздушном пространстве.

3.3.2 Страны пребывания, не являющиеся членами НАТО

(a) В толерантных условиях НАТО нацелена на достижение соглашения со страной пребывания, предусматривающего внешнюю защиту гражданских и военных органов НАТО. Данное соглашение будет включать те же условия и поддержку, оговоренные со страной пребывания в зоне ответственности НАТО, как описано в первой части настоящего документа.

(b) В полутолерантной среде со страной пребывания необходимо заключить подобные соглашения. Однако стране пребывания могут потребоваться средства и возможности для обеспечения/создания условий/поддержки, как было оговорено.

(c) В нетерпимой среде не следует ожидать поддержки со стороны страны пребывания.

3.3.3 Военачальники НАТО

Военачальники НАТО отвечают за:

(a) Планирование, включая оценку угроз, процесс принятия решений, координацию и реализацию контртеррористических мер.

(b) Проверку по командным инстанциям отсутствия факта угрозы силам и средствам НАТО со стороны местных лиц, работающих по найму.

(c) Принятие во внимание принципов безопасности, изложенных в Части 1 и 2 данного С-М, при процессе планирования каждого оперативного плана.

(d) В толерантной или полутолерантной среде начальники НАТО должны полностью принять во внимание вышеуказанные соглашения со страной пребывания, а также соответствующие обязанности стран пребывания и стран, предоставляющих войск.

(e) В нетерпимой среде поддержка страны пребывания переходит к начальникам НАТО. Однако, они должны гарантировать функционирование в рамках мандата в соответствии с утвержденным оперативным планом.

(f) Во всех обстоятельствах начальники НАТО гарантируют, что координация и обмен информацией будут производиться с привлечением всех сторон, например путем установления связи со страной пребывания, по обстоятельствам, и через командные инстанции со всеми странами, выделившими войска, и принимая во внимание существующие правила безопасности.

(g) Военачальники НАТО могут при необходимости усилить минимальные меры,

как указано в Приложении 2, для объявленного состояния тревоги, как указано в Приложении 1. Стратегический военачальник может по обстоятельствам устанавливать процедуры по отмене минимальных мер состояния тревоги.

3.3.4 Страны, выделившие войска

(a) Страны, выделившие войска наряду с НАТО, несут ответственность за обеспечение поддержки безопасности своим национальным силам. Это включает в себя проверки, гарантирующие, что местный персонал, нанятый на работу, не представляет угрозы для сил НАТО.

(b) В толерантной или полутолерантной среде страны, выделившие войска, отвечают за обмен информацией о террористической/подрывной угрозе/происшествии посредством связи НАТО по обстоятельствам.

(c) Силы НАТО будут действовать с использованием санкционированных правил применения силы. Страны, выделившие войска, могут ограничить правила применения силы для исполнения своими национальными силами. Командующий НАТО будет проинформирован о таких национальных ограничениях.

3.3.5 Офис безопасности НАТО

Офис безопасности НАТО должен осуществить проверку контртеррористических программ объектов/средств НАТО при проведении своих периодических проверок в пределах обязательного 18-месячного цикла проверок. Инспекционная группа Офиса безопасности НАТО будет осуществлять проверку и консультировать относительно адекватности контртеррористических разделов плана внутренней безопасности объекта /подразделения и способности объекта/средства реализовывать данные контртеррористические разделы. Там где это уместно, инспекционная группа Офиса безопасности НАТО также проконсультирует относительно адекватности контртеррористической подготовки и программы учений объекта/подразделения, которые поддерживают план внутренней безопасности.

3.3.6 Гражданские органы НАТО

Главы гражданских органов несут ответственность за развитие плана безопасности до развертывания персонала.

Главы гражданских органов гарантируют, что план безопасности разрабатывается во взаимодействии с Офисом безопасности НАТО и соответствующим начальником НАТО до какого-либо развертывания.

Персонал, развертываемый от гражданских органов, должен располагаться с военными силами НАТО при любой возможности. Когда это невозможно план безопасности должен затрагивать все аспекты защиты, изложенные в параграфе 3.4.1.

3.4 ДОКЛАД О ТЕРРОРИСТИЧЕСКОЙ ИЛИ ПОДРЫВНОЙ ДЕЯТЕЛЬНОСТИ

3.4.1 Доклады о террористической/подрывной угрозе или происшествии различными гражданскими или военными органами должен содержать следующее:

(a) Орган, от которого исходит информация;

(b) Характер последствий угрозы или происшествия;

(c) Предпринятые действия.

3.4.2 В целях обеспечения адекватной информации соответствующих органов о террористических/подрывных угрозах или реальных происшествиях необходимо докладывать следующим образом:

(a) Начальники НАТО должны докладывать в вышестоящий штаб по вертикали командной инстанции и своим подчиненным командирам;

(b) В целях обеспечения схожих мер безопасности силы стран, не являющихся членами НАТО, в операциях, проводимых НАТО, должны участвовать в системе доклада в соответствии с существующими соглашениями по безопасности;

(c) Все страны, выделившие войска, будут проинформированы об особой угрозе/ происшествии через своих командиров национальных контингентов на театре военных действий на следующих уровнях командования и/или в штабе НАТО;

(d) По обстоятельствам, власти страны пребывания должны проинформировать командиров НАТО и/или быть проинформированными об угрозе/происшествии через назначенного офицера связи НАТО по заблаговременной договоренности с данной страной и в соответствии с существующими правилами безопасности;

(e) Гражданские органы НАТО должны докладывать о своих контртеррористических и противодиверсионных мерах с общей оценкой угрозы через свои столицы в Офис безопасности НАТО.

3.5 ПЛАНИРОВАНИЕ И РЕАЛИЗАЦИЯ

3.5.1 Начальники НАТО несут ответственность за планирование и реализацию мер по борьбе с терроризмом и угрозами диверсии.

3.5.2 Главы объектов, гражданские органы НАТО, командиры штабов постоянной дислокации силовых структур должны разрабатывать план внутренней безопасности.

3.5.3 План внутренней безопасности включает в себя:

(a) Оценку угрозы терроризма/диверсии;

(b) Оценку управления рисками. Она должна включать, как минимум, оценку серьезности и уязвимости;

(c) меры безопасности, включая физическую безопасность;

(d) план реагирования на происшествие, который должен содержать:

(i) определение органа, ответственного за отдачу приказа на осуществление одной из стадий плана, и официальных лиц, несущих ответственность за реализацию особых мер, перечисленных в плане;

(ii) распределение обязанностей по командованию и управлению;

(iii) мероприятия на случай чрезвычайных ситуаций для сил поддержки и резервных сил;

(iv) описание действий сил безопасности НАТО в и за пределами помещений НАТО в соответствии с законодательством страны пребывания;

(v) альтернативные средства связи для сил безопасности;

(vi) особые действия и обязанности, связанные с применением каждой из мер по усилению бдительности;

(e) план ликвидации последствий, включающий:

(i) соответствующий персонал "первого реагирования", функцией которого является смягчить потерю/травматизм персонала и нанесение ущерба структурам/средствам. Персонал быстрого реагирования включает в себя, но не ограничивается: медицинским персоналом, пожарными и спасательными группами, подразделениями по деконтаминации оружия массового поражения (ОМП) и персоналом безопасности.

(ii) Соответствующее планирование осмотра места преступления правоохранительными органами, а также реагирования на потери персонала/ущерб собственности.

Персонал безопасности

3.5.4 Гражданские и военные органы НАТО должны принять во внимание контртеррористические и противодиверсионные соображения при установлении или проверке мер по охране их учреждений. Персонал по защите старших должностных лиц НАТО должен содержаться отдельно от других сил безопасности, а его развертывание должно координироваться с органами безопасности страны пребывания.

3.5.5 Гражданские и военные органы НАТО должны проводить подготовку своего персонала для выполнения своих функций в различных обстоятельствах путем официальных указаний и проведения учений с органами страны пребывания. Учения должны включать оповещение персонала в нерабочее время. В целях обеспечения эффективной реализации плана безопасности при необходимости чрезвычайно важно проводить подготовку задолго до прогнозируемой чрезвычайной ситуации.

Стандартная система оповещения

3.5.6 Стандартная система оповещения должна быть установлена во всех штабах гражданских и военных органов НАТО. Данная система оповещения должна состоять из четырех отдельных этапов, помимо обычных, и содержать основные минимальные меры, применяемые во всех гражданских и военных органах НАТО. Подробные данные относительно системы оповещения и соответствующей системы связи и основных минимальных мерах для каждой стадии, а также другие необходимые или рекомендуемые меры будут разрабатываться под эгидой Комитета безопасности НАТО (см. Приложение 1 "Состояния системы оповещения НАТО) и Приложение 2 " Состояния системы оповещения НАТО - минимальные меры").

СОСТОЯНИЯ ТРЕВОГИ БЕЗОПАСНОСТИ НАТО

1. ВВЕДЕНИЕ

Информация и предупреждения о террористической и подрывной деятельности, направленной против объектов и персонала гражданских и военных органов НАТО, может быть получена по тревоге НАТО либо через органы безопасности соответствующей страны пребывания. Информация может также поступать от местной полиции и напрямую быть получена гражданскими и военными органами НАТО в форме угрозы или предупреждения от террористической организации и, наконец, в качестве атаки на объект НАТО или персонал НАТО.

2. ЦЕЛЬ

Целью инструкций является разработать общую контртеррористическую систему тревоги для гражданских и военных органов НАТО и соответствующие меры реализации для каждого состояния тревоги.

3. СОСТОЯНИЯ ТРЕВОГИ

Обычные мероприятия по безопасности для защиты объектов, подразделений и баз НАТО (включая официальные резиденции, клубы, столовые и хозяйственные территории, т.е. незакрытые зоны) проводятся в соответствии с местным регламентом. Введение минимальных мер, изложенных в Состояниях тревоги (ПРИЛОЖЕНИЕ), отразит более высокую степень защиты безопасности, необходимой для борьбы с усилением террористической угрозы. Дополнительные меры для каждого стандартного состояния тревоги могут быть определены страной пребывания.

4. ОПРЕДЕЛЕНИЯ СОСТОЯНИЯ ТРЕВОГИ

4.1 Четыре состояния повышенной тревоги определяются следующим образом:

(a) состояние тревоги АЛЬФА.

Применяется, когда существует общая угроза возможной террористической деятельности, направленной против объектов и персонала НАТО, характер и степень которой непредсказуемы, а обстоятельства не оправдывают полное применение мер по состоянию тревоги "БРАВО". Однако возможно возникнет необходимость в применении определенных мер по состоянию "БРАВО" в соответствии с результатом полученных разведанных или в качестве средства предупреждения. Меры данного состояния тревоги должны поддерживаться неограниченно.

(b) состояние тревоги БРАВО.

Применяется при повышенной и более предсказуемой угрозе террористической деятельности. Данное состояние должно поддерживаться в течение нескольких недель, не вызывая несвоевременных трудностей, не оказывая влияния на оперативные возможности и не ухудшая отношения с местными властями.

(c) состояние тревоги ЧАРЛИ.

Применяется при происшествии или когда были получены разведанные, указывающие на то, что какая-либо форма террористической деятельности, направленная против объектов и персонала НАТО, является неизбежной. Реализация

данной меры на более длительный период, возможно, создаст трудности и повлияет на деятельность подразделения и персонала в мирное время.

(d) Состояние тревоги ДЕЛЬТА.

Применяется на территории, где произошла террористическая атака или были получены разведанные, гласящие, что вероятен теракт против определенного участка или человека. Обычно данное состояние тревоги объявляется в качестве локализированного предупреждения.

5. ОБЪЯВЛЕНИЕ СОСТОЯНИЯ ТРЕВОГИ И РЕАЛИЗАЦИЯ МЕР

5.1 Объявление состояний тревоги и реализация мер решается страной пребывания в зоне ответственности НАТО, гражданским или военным органом НАТО в результате полученных разведанных, либо местным начальником или главой агентства после получения разведанных через официальные источники или анонимного сообщения об угрозе.

5.2 Состояния тревоги могут быть дополнены географической зоной риска. Вся неофициальная информация должна всегда направляться, по обстоятельствам, органам безопасности страны пребывания для удостоверения подлинности.

6. ОРУЖИЕ И БОЕПРИПАСЫ

Местные приказы должны включать особые инструкции в отношении выдачи оружия и боевых патронов для охраны помещений и постов. Эти приказы должны соответствовать политике страны пребывания и гражданского или военного органа НАТО.

7. РЕАЛИЗАЦИЯ В ИНТЕГРИРОВАННЫХ ПОДРАЗДЕЛЕНИЯХ

Подробные меры, которые принимаются штабами НАТО на определенных территориях, где они делят помещения с национальными формированиями, будут скоординированы с последними.

8. КЛАССИФИКАЦИЯ СОСТОЯНИЙ ТРЕВОГИ

Полные определения состояний тревоги проходят под грифом "НАТО НЕСЕКРЕТНО" и могут использоваться по незащищенным телефонным линиям и посредством передачи сигнальных сообщений "НАТО НЕСЕКРЕТНО" (например, " Принять состояние ЧАРЛИ"). Это быстрый способ передачи исходной информации, за которым может следовать уточняющее сообщение, секретность которого зависит от его содержания (например, источник защиты).

СОСТОЯНИЯ ТРЕВОГИ БЕЗОПАСНОСТИ НАТО - МИНИМАЛЬНЫЕ МЕРЫ

1. СОСТОЯНИЕ ТРЕВОГИ АЛЬФА

Объявляется в качестве общего предупреждения возможной террористической деятельности, характер и степень которой непредсказуемы, и обстоятельства не оправдывают полное применение мер по состоянию тревоги БРАВО. Однако,

возможно возникнет необходимость в применении определенных мер по состоянию БРАВО.

М Е Р А 1 .

Весь персонал, включая членов семей, должен с регулярными интервалами относиться с подозрением к незнакомым людям, особенно если они несут чемоданы или другие предметы багажа; к неопознанным автомобилям на или около объектов НАТО; к оставленным посылкам или чемоданам или другой необычной деятельности.

М Е Р А 2 .

Дежурный офицер безопасности или другие назначенные офицеры должны всегда быть на связи с наличием доступа к плану эвакуации используемых зданий и территорий и блокированию территорий, где произошло нападение или взрыв. Ключевой персонал, который может быть необходим для реализации плана безопасности, должен всегда находиться на связи.

М Е Р А 3 .

Здания, комнаты и шкафы, которые нерегулярно используются, должны охраняться.

М Е Р А 4 .

Проведение усиленной выборочной проверки транспортных средств и людей, входящих на территорию объектов и несекретных зон, подконтрольных гражданскому или военному органу НАТО.

М Е Р А 5 .

Ограничить точки доступа транспортных средств и персонала до минимума, соизмеримого с разумным потоком движения.

М Е Р А 6 .

Одна из нижеследующих мер из состояния БРАВО должна индивидуально и нерегулярно применяться в качестве сдерживающего фактора:

(a) все здания, комнаты и шкафы нерегулярного использования должны охраняться и регулярно проверяться. (мера 14).

(b) внешняя и внутренняя части зданий регулярного использования должны регулярно и часто проверяться на наличие подозрительной деятельности или тар. (мера 15).

(c) все доставки в клубы/столовые должны проверяться. (членам семей будет рекомендовано сделать то же самое с доставками на дом) (мера 17).

(d) насколько это позволяют ресурсы, наблюдение за местами проживания, кафе, школами, клубами и другими доступными целями должно быть усилено для улучшения сдерживания, обороны и уверенности среди персонала и членов семей (мера 18).

М Е Р А 7 .

Просмотреть все планы, приказы, данные о персонале и материально-технические требования, связанные с введением более высоких степеней тревоги.

М Е Р Ы 8 - 9 .

Резервные.

2. СОСТОЯНИЕ ТРЕВОГИ БРАВО

Объявляется при повышении и более предсказуемом характере угрозы террористической деятельности, несмотря на то, что не было установлено какой-либо определенной цели.

М Е Р А 1 0 .

Меру 1 следует повторить, а персонал предупредить о любой другой форме нападения, используемой террористами.

М Е Р А 1 1 .

Все офицеры, участвующие в реализации планов по контртеррористической деятельности, должны быть на связи.

М Е Р А 1 2 .

Планы по реализации мер, содержащихся в следующих состояниях тревоги, должны проверяться.

М Е Р А 1 3 .

Где это возможно, машины и такие объекты как: ящики мусорные ящики и т.д.; должны быть перемещены, по крайней мере, на расстояние около 25 метров от зданий, в особенности секретных. Рассмотреть применение централизованной парковки.

М Е Р А 1 4 .

Все здания, комнаты и шкафы нерегулярного использования должны охраняться и регулярно проверяться.

М Е Р А 1 5 .

Внешняя и внутренняя части зданий регулярного использования должны постоянно и часто проверяться на подозрительные тары и всегда в начале, и в конце рабочего дня.

М Е Р А 1 6 .

Вся почта должна определенно проверяться на наличие бомб в письме/посылке (усилить проверки).

М Е Р А 1 7 .

Все доставки в столовые, клубы и т.д. должны проверяться. (членам семей будет рекомендовано сделать то же самое с доставками на дом).

М Е Р А 1 8 .

Насколько это позволяют ресурсы, наблюдение за местами проживания, кафе, школами, клубами и другими доступными целями должно быть усилено для улучшения сдерживания, обороны и уверенности среди персонала и членов семей.

М Е Р А 1 9 .

Персонал и члены семей должны быть осведомлены об общей обстановке для прекращения слухов и предупреждения тревоги.

М Е Р А 2 0 .

Члены местных комитетов безопасности должны быть информированы на ранней стадии о каких-либо предпринимаемых действиях и причинах.

М Е Р А 2 1 .

Посетители подразделения и определенный процент их сумок, посылок и других видов багажа должны выборочно проверяться на входе.

М Е Р А 2 2 .

Везде где возможно должны работать выборочные патрули по проверке транспортных средств, людей и зданий.

М Е Р А 2 3 .

Персонал и служебный транспорт, находящийся вне базы, должен охраняться в соответствии с подготовленными планами. Водителям необходимо напомнить о закрывании припаркованных автомобилей и ввести установленную систему проверки до того, как они сядут в машину и начнут вождение.

М Е Р Ы 2 4 - 2 8 .

Резервные.

3. СОСТОЯНИЕ ТРЕВОГИ ЧАРЛИ

Применяется при происшествии или при получении разведанных, указывающих на то, что какая-либо форма террористической деятельности, является неизбежной.

М Е Р А 2 9 .

Охрану необходимо усилить по мере необходимости.

М Е Р А 3 0 .

Принятие всех мер по состоянию БРАВО необходимо продолжить либо ввести дополнительные.

М Е Р А 3 1 .

Все офицеры, отвечающие за реализацию контртеррористических планов, должны находиться на месте службы.

М Е Р А 3 2 .

Ограничение пунктов доступа до абсолютного минимума.

М Е Р А 3 3 .

Усилить контроль за входом и проводить выборочные проверки транспортных средств.

М Е Р А 3 4 .

Ввести централизованную парковку транспортных средств в отдалении от важных зданий.

М Е Р А 3 5 .

Выдача оружия охране. (Местные приказы должны включать особые инструкции по выдаче боеприпасов).

М Е Р А 3 6 .

Необходимо ввести усиленное патрулирование объекта.

М Е Р А 3 7 .

Все отмеченные уязвимые объекты должны охраняться, и особое внимание следует уделить уязвимым объектам, не установленным на военных базах.

М Е Р А 3 8 .

Установить лежачие заграждения для контроля транспортных средств.

М Е Р А 3 9 .

Минимизировать присутствие персонала из числа местного населения.

М Е Р А 4 0 .

Охрану усилить по мере необходимости.

4. СОСТОЯНИЕ ТРЕВОГИ ДЕЛЬТА

Данные меры применяются на территории, где произошла террористическая атака или были получены разведанные, согласно которым существует вероятность теракта против определенного участка или человека. Обычно данное состояние тревоги объявляется в качестве локализированного предупреждения.

М Е Р А 4 1 .

Принятие всех мер, перечисленных в состояниях тревоги БРАВО и ЧАРЛИ, продолжается или начинается.

М Е Р А 4 2 .

Все транспортные средства, находящиеся на базе, идентифицируются.

М Е Р А 4 3 .

Все транспортные средства и их содержимое, въезжающие на территорию комплекса или объекта, обыскиваются.

М Е Р А 4 4 .

Доступ полностью контролируется.

М Е Р А 4 5 .

Все сумки, портфели, упаковки и т.д., вносимые на территорию комплекса или объекта, обыскиваются.

М Е Р А 4 6 .

Должны быть приняты меры по контролю доступа во все зоны подконтрольные соответствующему гражданскому или военному органу НАТО.

М Е Р А 4 7 .

Необходимо проводить частые проверки внешней части зданий и стоянок.

М Е Р А 4 8 .

Свести к минимуму все административные поездки и визиты.

М Е Р А 4 9 .

Проконсультироваться с местными властями относительно вопроса закрытия

общественных (и военных) дорог, которые могут сделать объекты уязвимыми к террористической атаке.

МЕРА 50.

Резервная.

СЛОВАРЬ

Противо-диверсионный/ противоподрывной	Действие, предпринимаемое для обнаружения и противодействия диверсии (источник: AAP-6).
Контртерроризм	Меры, предпринимаемые для предупреждения, удержания и реагирования на терроризм в целях снижения уязвимости индивидов и средств к теракту.
Средство/актив НАТО	Средства/активы НАТО - это те средства, структуры, оборудование и другие предметы, включая системы и ресурсы, которые играют важную роль в выполнении миссии НАТО.
Диверсия	Действия, направленные на затруднение миссии НАТО путем преднамеренного повреждения или уничтожения средств НАТО.
Терроризм	Незаконное использование или угроза использования силы или насильственных действий против индивидов или имущества в попытке принуждения или запугивания правительств или обществ в целях достижения политических, религиозных или идеологических задач. (Источник: AAP-6)

Текст переведен на русский язык в соответствии с оригиналом.

Начальник Главного управления международных программ Вооруженных Сил Республики Казахстан

полковник В. Райхель

СОГЛАШЕНИЕ О БЕЗОПАСНОСТИ МЕЖДУ РЕСПУБЛИКОЙ КАЗАХСТАН И ОРГАНИЗАЦИЕЙ СЕВЕРОАТЛАНТИЧЕСКОГО ДОГОВОРА

СОГЛАШЕНИЕ О БЕЗОПАСНОСТИ

Правительство Республики Казахстан,

представленное Послом Ауесханом Кырбасовым, Постоянным представителем в Штаб-квартире НАТО

Организация Североатлантического Договора,
представленная Хавьером Соланой, Генеральным секретарем Организации Североатлантического Договора

Признавая, что Республика Казахстан является страной-партнером в Совете Североатлантического Сотрудничества (ССАС)/Партнерстве во имя мира (ПИМ);

Согласившись проводить консультации по политическим вопросам и по проблемам безопасности, и расширять и усиливать политическое и военное сотрудничество в Европе;

Осознавая, что для эффективного сотрудничества в этой области необходим обмен чувствительной и/или привилегированной информацией между сторонами;

Согласились о следующем:

Статья 1

Стороны будут:

(i) защищать и охранять информацию и сведения другой Стороны;

(ii) делать все необходимое для обеспечения того, чтобы секретная информация и сведения содержали условия допуска, определенные любой из Сторон с учетом информации и сведений другой Стороны, и защищать такую информацию и сведения по согласованным общим стандартам;

(iii) не использовать обмениваемую информацию и сведения для целей, не предусмотренных рамками соответствующих программ, а также решениями и резолюциями, имеющими отношение к этим программам;

(iv) не предоставлять такую информацию и сведения третьим сторонам без согласия источника информации.

Статья 2

(i) Правительство Республики Казахстан принимает на себя обязательство соответствующим образом оформить допуск всех своих граждан, имеющих по своим профессиональным обязанностям доступ к информации и сведениям, полученным в рамках ССАС или ПИМ, до того, как они получат доступ к такой информации и сведениям.

(ii) Процедуры оформления допуска должны проходить таким образом, чтобы определить, может ли человек, принимая во внимание его лояльность и надежность, иметь доступ к такой информации без риска для ее секретности.

Статья 3

Офис НАТО по безопасности (NOS) под управлением и от лица Генерального Секретаря и Председателя, Военного Комитета НАТО, действуя от имени Северо-Атлантического Совета и Военного Комитета НАТО и согласно их указаниям, ответственен за вопросы безопасности и защиты секретной информации, обмениваемой в рамках ССАС/ПИМ.

Статья 4

Республика Казахстан будет информировать NOS о национальных органах безопасности со схожими функциями. Отдельные Административные Условия будут разработаны между Правительством Республики Казахстан и НАТО, которые включат, кроме всего прочего, стандарты взаимной защиты безопасности обмениваемой информации и связи между органами Республики Казахстан и NOS.

Статья 5

До обмена любой секретной информацией между Правительством Республики Казахстан и НАТО, ответственные органы безопасности должны взаимно убедиться, что сторона-получатель готова обеспечить защиту информации, которая она получает, согласно требованиям отправителя.

В свидетельство чего упомянутые выше Представители подписали настоящее Соглашение.

Подписано в двух экземплярах в Брюсселе 31 июля 1996 года на английском и французском языках, имеющих одинаковую силу.

За Правительство Республики Казахстан
Ауесхан Кырбасов

За Организацию Североатлантического Договора
Хавьер Солана

Настоящим удостоверяю, что данный текст является неофициальным переводом на русский язык Соглашения о безопасности между Республикой Казахстан и Организацией Североатлантического Договора, совершенного в городе Брюссель 31 июля 1996 года.

Начальник Главного управления международных программ Вооруженных Сил Республики Казахстан
полковник В. Райхель

ПАРТНЕРСТВО ВО ИМЯ МИРА: РАМОЧНЫЙ ДОКУМЕНТ

1. В дополнение к приглашению, с которым главы государств и правительств стран-членов НАТО выступили на своей встрече 10-11 января 1994 года, государства-члены Североатлантического союза и другие государства, подписавшие этот документ и выразившие решимость углублять политические и военные связи и способствовать дальнейшему укреплению безопасности в Евро-Атлантическом районе, настоящим учреждают на основе Совета Североатлантического сотрудничества это "Партнерство во имя мира".

2. Это партнерство является выражением совместной убежденности, что стабильность и безопасность в Евро-Атлантическом районе могут быть достигнуты только на основе сотрудничества и совместных действий. Защита и поддержка основных свобод и прав человека и обеспечение свободы, справедливости и мира на принципах демократии являются общими ценностями, основополагающими для этого партнерства. Присоединяясь к этому партнерству, государства-члены Североатлантического союза и другие государства, подписавшие этот документ, напоминают, что они привержены сохранению демократических обществ, их свободы от принуждения и устрашения и поддержанию принципов международного права. Они подтверждают свою приверженность добросовестному соблюдению обязательств, вытекающих из Устава ООН и принципов Всеобщей декларации прав человека; и конкретно обязательств воздерживаться от угрозы применения силы и от применения силы в ущерб территориальной целостности или политической независимости любого государства, а также уважать существующие границы и добиваться урегулирования споров мирными средствами. Они также подтверждают свою приверженность Хельсинкскому Заключительному акту и всем последующим документам СБСЕ, а также соблюдению обязательств; принятых ими на себя в области разоружения и контроля над вооружениями.

3. Другие государства, подписавшие этот документ, будут сотрудничать с Организацией Североатлантического договора во имя достижения следующих целей:

(а) содействия транспарентности в планировании национальной обороны и разработке бюджетов;

(б) обеспечения демократического контроля над силами обороны;

(в) поддержания способности и готовности вносить вклад с учетом положений национальных конституций в операции под эгидой ООН и/или СБСЕ;

(г) установления в военной области основанных на сотрудничестве отношений с НАТО в целях совместного планирования, боевой подготовки и проведения учений для повышения их готовности к проведению операций в областях миротворчества, поиска и спасения, гуманитарных и других операций, о которых впоследствии может быть достигнута договоренность;

(д) формирования в долгосрочной перспективе сил, в большей степени готовы к взаимодействию с вооруженными силами стран-членов Североатлантического союза.

4. Другие государства, подписавшие этот документ, представят руководству НАТО презентационные документы, в которых будут изложены меры, намечаемые ими для достижения политических целей партнерства, и военные и другие активы, которые могут быть использованы для деятельности по программе этого партнерства, НАТО предложит программу учений на принципе партнерства и других видов деятельности, отвечающих целям партнерства. На основе этой программы и своего презентационного документа каждое государство, подписавшее этот документ, будет разрабатывать вместе с НАТО индивидуальную программу партнерства.

5. В ходе подготовки и проведения в жизнь индивидуальных программ партнерства другие государства, подписавшие этот документ, могут на свои средства и на основе соглашения с Североатлантическим союзом и, если потребуется, соответствующими бельгийскими властями, учредить свои бюро связи со штаб-квартирой НАТО в Брюсселе. Это облегчит для них участие во встречах и деятельности Совета Североатлантического сотрудничества и "Партнерства во имя мира", а также некоторых других на основе приглашения. Кроме того, они выделят и предоставят персонал, активы, оборудование и возможности, необходимые для выполнения согласованной программы партнерства. НАТО окажет им надлежащую помощь в разработке и проведении в жизнь их индивидуальных программ партнерства.

6. Другие подписавшие документ государства соглашаются со следующим:

- Те, кто рассчитывает принимать участие в операциях, о которых говорится в параграфе 3 (г), будут, когда это возможно, участвовать в учениях НАТО в соответствующих областях;

- Они будут сами финансировать свое участие в деятельности по программе " Партнерства во имя мира" и будут предпринимать другие усилия с тем, чтобы взять на себя часть бремени проведения учений, в которых они будут принимать участие;

- Возможно они направят после достижения надлежащей договоренности постоянных офицеров связи в отдельную Группу координации партнерства в Монсе (Бельгия), которая под руководством Североатлантического совета будет заниматься военным планированием, необходимым для проведения в жизнь программ партнерства;

- Те, кто будет принимать участие в планировании и военных учениях, получать доступ к некоторым техническим данным НАТО, необходимым для взаимодействия;

- На основе мер, предусмотренных СБСЕ в области военного планирования, другие государства, подписавшие документ, и страны НАТО будут обмениваться информацией о шагах, предпринятых или предпринимающихся для содействия обеспечению транспарентности в военном планировании и при подготовке бюджетов, а также в обеспечении демократического контроля над вооруженными силами;

- Они могут принимать участие во взаимном обмене информацией в области военного планирования и подготовки бюджетов, который будет осуществляться в

рамках Совета Североатлантического сотрудничества/Партнерства во имя.

7. На основе приверженности целям этого "Партнерства во имя мира", члены Североатлантического союза будут:

Развивать вместе с другими государствами, подписавшими документ, процесс планирования и исследований в целях закладки основы для выявления и оценки сил и мощностей, которые могут быть предоставлены ими для международной боевой подготовки, учений и операций во взаимодействии с силами Североатлантического союза;

Содействовать военной и политической координации в штаб-квартире НАТО, чтобы обеспечить руководство и управление соответствующей деятельностью на основе партнерства с другими государствами, документ подписавшими, включая планирование, боевую подготовку, учения и разработку доктрины.

8. НАТО будет проводить консультации с любым активным участником партнерства, если этот партнер сочтет, что существует прямая угроза его территориальной целостности, политической независимости или безопасности.

Настоящим удостоверяю, что данный текст является неофициальным переводом на русский язык Рамочного документа: "Партнерство во имя мира" от 27 мая 1994 года, опубликованного в "Сборнике документов по международному праву" под обшей редакцией К.К. Токаева. Алматы: изд. АО "Сак", Т.I, стр. 300-302.

Начальник Главного управления
международных программ
Вооруженных Сил Республики Казахстан
полковник *В. Райхель*

Неофициальный перевод

ПАРТНЕРСТВО ВО ИМЯ МИРА: ПРИГЛАШЕНИЕ

Одобрено Главами государств и правительств, участвовавших на Совещании Североатлантического Совета, проведенном в штаб-квартире НАТО, 10-11 января 1994 года в Брюсселе

Мы, главы государств и правительств стран-членов Североатлантического союза, основываясь на тесном и долгосрочном партнерстве между Североатлантическими и Европейскими союзниками, выполняем обязательства по укреплению безопасности и стабильности во всей Европе. Поэтому мы намерены укрепить связи с демократическими государствами на Востоке. Мы вновь подтверждаем, что Альянс, как предусмотрено в Статье 10 Вашингтонского договора, остается открытым для членства других Европейских государств в вопросах продвижения принципов Договора и достижения безопасности в Северо-Атлантическом регионе. Мы ожидаем и приветствуем расширение НАТО, которое достигло бы демократических государств на

Востоке, как часть эволюционного процесса, учитывая политические достижения и достижения в области безопасности по всей Европе.

Сегодня мы инициировали безотлагательную и практическую программу, которая изменит взаимоотношения между НАТО и участвующими странами. Эта новая программа выходит за рамки диалога и взаимодействия, продвигая настоящее партнерство - Партнерство во имя мира. Поэтому мы приглашаем другие государства, входящие в Совет Североатлантического сотрудничества, а также страны, принимающие участие в Совещании по безопасности и сотрудничеству в Европе (СБСЕ), которые готовы и имеют желание внести вклад в эту программу, присоединиться к нам в этом партнерстве. Активное участие в программе " Партнерство во имя мира" сыграет огромную роль в эволюционном процессе по расширению НАТО.

Программа "Партнерство во имя мира", которая будет действовать под руководством Североатлантического союза, создаст новые отношения безопасности между Североатлантическим союзом и его партнерами во имя мира. Страны - партнеры будут приглашаться Североатлантическим Советом для работы в политических и военных органах в штаб-квартирах НАТО в соответствии с деятельностью Партнерства . Партнерство будет способствовать расширению и усилению политического и военного сотрудничества по всей Европе, повышать уровень стабильности, уменьшит угрозы миру, а также строить прочные взаимоотношения путем повышения духа практического сотрудничества и приверженности к демократическим принципам, которые лежат в основе нашего Союза. НАТО будет консультировать любого активного участника Партнерства, в случае возникновения прямой угрозы его территориальной целостности, политической независимости или его безопасности. В темпе и масштабе, определяемых возможностями и желанием каждого государства-участника, мы будем осуществлять конкретные мероприятия по достижению прозрачности военного финансирования по расширению рамок демократического контроля над деятельностью военных ведомств, совместному планированию и проведению совместных военных учений в целях взаимодействия с силами НАТО в операциях по поддержанию и установлению мира, поисково-спасательных, гуманитарных и других мероприятиях по соответствующему согласованию.

В целях достижения более тесного сотрудничества и взаимопонимания, мы предлагаем в рамках программы Партнерства, начать проведение миротворческих полевых учений в 1994 году. Для координации совместных военных действий в рамках Партнерства, мы будем приглашать государства-участники направлять постоянных офицеров связи в штаб-квартиры НАТО, а также в отдельный Центр координации партнерства в Монсе (Бельгия), которые будут, под руководством Североатлантического Совета, осуществлять военное планирование, необходимое для

осуществления программ Партнерства.

Со времени создания два года назад, Совет евроатлантического сотрудничества значительно расширил масштабы своей деятельности. Мы намерены продолжать работу со всеми государствами, входящими в Совет евроатлантического сотрудничества, для создания взаимовыгодного сотрудничества по всем мероприятиям, проводимым Союзом. С расширением деятельности Совета евроатлантического сотрудничества, а также с созданием программы "Партнерство во имя мира", мы решили выделить постоянные помещения в штаб-квартире НАТО для персонала стран, входящих в ССАС и других участников программы "Партнерство во имя мира", для качественного улучшения рабочих отношений и установления более тесного сотрудничества.

В соответствии с приглашением к участию в "Партнерстве во имя мира", одобренном и подписанном главами государств и правительств государств участников Организации Североатлантического договора, участвовавших в совещании Североатлантического совета, проведенном в штаб-квартире НАТО в Брюсселе 10-го и 11-го января 1994 года,

Я нижеподписавшийся, Министр иностранных дел Республики Казахстан, настоящим принимаю приглашение к участию в Партнерстве во имя мира и подписываю рамочный документ Партнерство во имя мира.

Подписано в Брюсселе, 27-го мая 1994 года.

(подписано)
Канат Саудабаев

Настоящим удостоверяю, что данный текст является неофициальным переводом на русский язык Приглашения к Партнерству во имя мира, подписанного 27 мая 1994 года.

Начальник Главного управления международных программ Вооруженных Сил Республики Казахстан

полковник В. Райхель

Примечание РЦПИ: далее прилагается текст Меморандума о понимании между Казахстаном и Организацией НАТО по техническому обслуживанию и обеспечению (НАМСО) по сотрудничеству в области материально-технического обеспечения на английском языке.