

**РАЗВЕДКА В ОТКРЫТЫХ ИСТОЧНИКАХ
OPEN-SOURCE INTELLIGENCE (OSINT)
«АТР 2-22.9»**

Содержание:

Вступительное слово

Введение

Глава 1. Основные принципы разведки в открытых источниках

Основные понятия и термины

Характеристики

Функций разведки при боевых операциях

Процесс ведения разведки

Требования к планированию и оценка процесса сбора информации

Процесс принятия решений

Разведывательная подготовка к боевым действиям

Глава 2. Планирование и подготовка разведки в открытых источниках

Раздел I – Планирование деятельности OSINT

Определение операционной среды

Описание влияния внешних факторов на проведение операции

Оценка угроз

Определение сценариев развития угроз

Раздел II – Подготовка процесса ведения разведки в открытых источниках

Ведение разведки в открытых источниках

Подготовка к проведению OSINT

Раздел III – Факторы, влияющие на процесс планирования и подготовки

Надежность открытых источников

Достоверность содержания информации в открытых источниках

Соответствие

Мероприятия по обеспечению безопасности

Гриф секретности

Координация

Дезинформация

Авторское право и интеллектуальная собственность

Лингвистические требования

Автоматизированная система перевода иностранных языков

Раздел IV – Комплектование личного состава подразделений OSINT

Обязанности подразделения OSINT

Подразделение OSINT на уровне бригадно-тактической группы

Глава 3. Сбор разведывательных данных из открытых источников

Сбор общедоступной информации

Исследование данных

Глава 4. Проведение разведки в открытых источниках

Категорий разведывательных данных

Анализ информации

Процесс обработки информации

Процесс предоставления и распространения информации

Факторы, влияющие процесс предоставления и распространения

Приложение А

Законодательные и нормативные ограничения

Приложение В

Осведомленность по вопросу кибербезопасности

Приложение С

Основные и продвинутые методы поиска информации в Интернете

Приложение D

Польза разведки в открытых источниках

Приложение E

Организаций, занимающиеся разведкой в открытых источниках

Приложение F

Ресурсы открытых источников

ВСТУПИТЕЛЬНОЕ СЛОВО

«АТР 2-22.9» устанавливает общие понятия, основные концепции и методы сбора разведывательных данных из открытых источников для Армии США.

«АТР 2-22.9» подчеркивает характеристику OSINT как разведывательной дисциплины, его связи с другими разведывательными дисциплинами, и возможности его применения в ходе объединенных операций.

Данный доклад:

- Указывает основные принципы и терминологию, которые подразделения Сухопутных войск США используют при планировании и проведении разведки в открытых источниках;

- Обсуждает тактику, технику (методы) и процедуры подразделений, занимающихся планированием проведения операций по разведке в открытых источниках;

- Подчеркивает важность общедоступной информации из открытых источников;

- Определяет общие понятия ведения разведки в открытых источниках.

- Разрабатывает систематизированные методы по планированию, подготовке, сбору, анализу и обработке разведывательных данных, полученных в результате ведения разведки в открытых источниках;

Целевой аудиторией данной разработки являются подразделения Армии США, находящиеся на уровне дивизии и ниже и занимающиеся разработкой и проведением OSINT.

Определения и термины указаны в тексте. Определения, применяемые в данной публикации, выделены жирным шрифтом.

Термин «персонал OSINT» применяется в отношении разведывательного и не разведывательного персонала Армии, Национальной гвардии, кадрового резерва США, которые активно участвуют в миссиях по обработке информации, поступающей из открытых источников.

«AR 381-10» определяет персонал США:

- гражданин США;
- постоянного иностранного резидента;
- неакционерная ассоциация, состоящая из граждан США или иностранных резидентов;
- корпорации или дочерние компании, функционирующие в США и не находящиеся под руководством или контролем иностранного правительства.

Не принято считать персоной США:

- человека, находящегося за пределами США;
- человек, не являющийся гражданином или постоянным резидентом США.

Использование или упоминание Сухопутными войсками в докладе какой-либо частной или коммерческой организации, а также связанных с ними торговых марок и услуг, не означает, что Вооруженные силы рекламируют данные организации.

Данная публикация распространяется только на подразделения действующей Армии, Национальной гвардии и кадровый резерв ВС США, за исключением особых указаний.

ВВЕДЕНИЕ

До создания спутников и других современных технологий, предназначенных для сбора разведданных, военные осуществляли планирование, сбор, обработку и подготовку разведывательных данных на основе общественно-доступной информации из открытых источников. Разведка в открытых источниках также ведется в целях сбора сведений и полного понимания территории, населения, потенциальных угроз и вооруженных сил иностранных государств.

Открытые источники содержат огромное количество информации, соответствующей требованиям разведывательного органа и необходимой для полного понимания физических и человеческих факторов оперативной обстановки на местах проведения объединенных наземных операций. Следует отметить, что для повышения эффективности разведывательной деятельности необходимо использовать общедоступную информацию в комплексе с техническими и оперативными ресурсами.

Мировое сообщество все больше использует информацию из открытых источников в целях решения широкого спектра задач. Значимость и актуальность сбора разведданных из открытых источников служит в качестве экономии сил, создания дополнительных возможностей и условий для уточнения или

перепроверки поступающей информации и разведанных.

Разведка в открытых источниках OSINT является одним из способов ведения разведки, вносит значительный вклад при планировании боевых действий, а также обеспечивает всей необходимой информацией при ее проведении.

ГЛАВА 1

ОСНОВНЫЕ ПРИНЦИПЫ ВЕДЕНИЯ РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ

Инициаторы и преобразующие директивы привели к принятию законодательства, которое повлияло на деятельность разведывательного сообщества США, в частности активизировалось использование общедоступной информации. Реформы разведсообщества США начались с принятия Закона о национальной безопасности в 1992 г., результатом которого стало создание Управления разведки в открытых источниках, которое в 2005 г. было преобразовано в Центр разведки в открытых источниках (OSC) под руководством Директора национальной разведки (DNI).

Данная глава описывает основные методы сбора информации из открытых источников (OSINT).

ОСНОВНЫЕ ПОНЯТИЯ И ТЕРМИНЫ

1-1. *Разведка в открытых источниках (OSINT)* является одним из методов ведения разведки путем сбора информации из открытых источников, ее анализа, подготовки и своевременного предоставления конечного продукта вышестоящему руководству в целях решения определенных разведывательных задач.

1-2. OSINT является методом ведения разведки, разработанным на основе сбора и анализа общедоступной информации, и не находящимся под непосредственным контролем правительства США. OSINT является результатом систематизированного сбора, обработки и анализа необходимой общедоступной информации.

Существует два важных термина:

Исследовательский Центр Виктора Воксанаева
Бюллетень OSINT № 33 (сентябрь – октябрь 2013 г.)

- **Открытый источник** – это персона или группа, которая предоставляет информацию без требования сохранения ее конфиденциальности – информация или отношения незащищенные от публичного раскрытия. Открытый источник информации может быть общедоступным, но не вся публично доступная информация является открытым источником. Открытые источники относятся к среде общедоступной информации, и не имеют ограничения в доступе для физических лиц.

- **Общедоступная информация** - данные, факты, инструкции или другие материалы, опубликованные или размещенные для широкого использования; доступные для общественности; законно увиденные или услышанные случайными наблюдателями; или представленные на открытых встречах для общественности.

1-3. OSINT обычно осуществляется с помощью мониторинга, анализа и исследования информации из сети Интернет. Материалы, составленные на основе информации из открытых источников, поддерживают все методы ведения разведки и разведывательные мероприятия путем накопления разведывательных знаний, анализа и их распространения. Аналогично с другими методами ведения разведки, направленность деятельности подразделений OSINT зависит от информационно-разведывательных требований командиров.

ХАРАКТЕРИСТИКИ

1-4. Нижеперечисленные характеристики определяют роль OSINT при проведении объединенных наземных операции:

- **Обеспечение основы.** Большая часть необходимых справочных материалов о районах проведения операции добывается из открытых источников. Эта основа достигается путем сбора информации из СМИ, которые освещают международные события и реакцию неамериканских сообществ. Накопление разведывательных данных из открытых источников является основной функцией подразделений OSINT.

- **Соответствие требованиям.** Доступность, глубина и масштабы публично доступной информации позволяют разведывательным органам находить необходимую информацию без привлечения специализированных человеческих и технических средств разведки.

- **Упрощение процессов сбора разведанных.** Исследование с использованием открытых источников поддерживает мероприятия по

наблюдению и рекогносцировке, в то же время, отвечает информационно-разведывательным требованиям. OSINT предоставляет информацию (например: биография, культура населения, геопространственная информация и технические данные), тем самым, исключая необходимость привлечения излишних технических и человеческих методов ведения разведки.

-Увеличение производительности. Являясь частью разведывательного процесса, OSINT позволяет руководству осуществлять глубокий анализ общедоступной информации в целях принятия соответствующих решений.

ФУНКЦИИ РАЗВЕДКИ ПРИ БОЕВЫХ ОПЕРАЦИЯХ

1-5. Существуют четыре основные тактические задачи разведывательных подразделений Сухопутных войск США при подготовке и проведении боевых операции:

- Разведывательная поддержка при формировании войск;
- Обеспечение ситуационной осведомленности;
- Ведение разведки, наблюдения и рекогносцировки;
- Оказание помощи при выборе целей и обеспечения информационного превосходства.

1-6. Функций разведки в ходе боевых операций – комплекс задач и систем, способствующих к быстрому пониманию среды ведения боевых операций, противника, рельефа местности, погодных условий и человеческого фактора. Они включают в себя анализа информации из всех источников в целях осуществления прогноза развития ситуации. OSINT поддерживает каждую из вышеуказанных функций.

1-7. Общедоступная информация используется для:

- Обеспечения ситуационного понимания потенциальных угроз и оперативной обстановки;
- Получения сведений о характере угроз, рельефе местности, погодных условиях и человеческом факторе;
- Накопления и анализа разведывательных данных в целях предоставления необходимой информации о местности проведения операции;
- Своевременного предоставления кратких разведывательных справок по интересующим руководство вопросам;
- Предоставления основной информации, при составлении общей разведывательной справки о месте проведения операции, потенциальных угрозах и намерениях противника;

- Создания базы разведданных Сухопутных войск, предназначенной для осуществления эффективной разведывательной подготовки боевых операций (IPB). Разведывательная подготовка боевых операций создана для штабной оценки и оказания содействия процессу принятия решения военным руководством (MDMP). Основные требования к разведке были сформированы в результате существующей необходимости разведывательного обеспечения боевых операций и взаимосвязи с процессом принятия решений.

- Прогнозирования развития ситуации. Прогнозирование -это процесс анализа доступной информации и составление разведывательных оценок по развитию ситуации, возможных сценариев, действий противника, рельефа местности, погодных условий и человеческого фактора до и в ходе проведения операции.

Изучение оперативной обстановки:

- Помогает офицерам отдела разведки/помощнику начальника штаба по разведке (G-2/S-2) в процессе определения угроз, намерений и целей;

- Помогает определить возможные сценарий развития ситуации;

- Обеспечивает оценку угроз боевой эффективности;

- Поддерживает процесс сбора информации.

Требования к планированию и оценка методов сбора данных способствуют анализу информационных требований и выявлению «пробелов» в полученных данных, а также позволяет определить какие средства или комбинации необходимо использовать для соответствия данным требованиям.

1-8. Для получения более детальной информации о функциях разведки в ходе боевых действий посмотрите «Инструкцию ведения разведки в полевых условиях» (FM 2-0). Примеры того, как OSINT оказывает поддержку другим видам разведки и боевым задачам указаны в приложении D.

ПРОЦЕСС ВЕДЕНИЯ РАЗВЕДКИ

1-9. Процесс ведения разведки состоит из четырех этапов (планирования, подготовки, сбора и производства конечного материала) и четырех постоянных действий (анализа, накопления разведданных, оценки и распределения по направлениям). Процесс ведения разведки, также как и процессы подготовки боевых операций (планирование, подготовка, выполнение и подведение итогов), пересекаются и повторяются в соответствии с требованиями миссии.

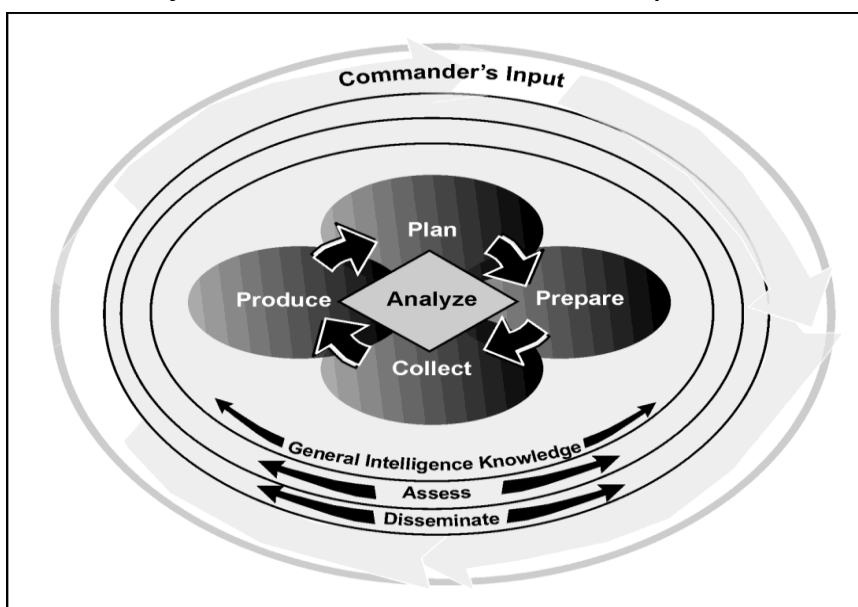
1-10. Четыре этапа постоянной деятельности по ведению разведки в соответствии с требованиями командира продвигают, формируют и развивают

процессы проведения разведывательных операций. Процесс ведения разведки предоставляет общую модель, которая формирует процессы мышления, рассмотрения различных ситуаций, планирования и составления прогнозов сотрудниками разведывательных органов.

1-11. Как указано в «Инструкции по ведению разведки в полевых условиях», OSINT повышает эффективность и оказывает поддержку процессу ведения разведки и других операций.

Процесс ведения разведки систематизирует ведение разведки в открытых источниках Сухопутными войсками, а также интегрирует механизм OSINT со структурами различных организаций (объединенных, межведомственных, межправительственных и межгосударственных).

Рисунок 1-1. Разведывательный процесс



ТРЕБОВАНИЯ К ПЛАНИРОВАНИЮ И ОЦЕНКА ПРОЦЕССА СБОРА ИНФОРМАЦИИ

1-12. Сбор информации позволяет руководству принять правильное

решение, оценить размеры необходимой боевой силы, а также последствия ее применения.

Сбор разведданных синхронизирует и интегрирует процессы планирования, использования технических средств, обработки и распределение системы для поддержки текущих и будущих боевых операций, что является объединенной разведывательной и оперативной функцией. Для Сухопутных войск данная функция является комбинированной боевой операцией, которая фокусирует основное внимание на первостепенной потребности в разведывательных данных и отвечает требованиям руководства по предоставлению особо важной информации.

1-13. После анализа, информация, полученная из различных источников, становится разведданными, которые содержат необходимую для руководства информацию о противнике, угрозах, климате, погодных условиях, рельефе местности и населению.

Разработка разведывательных требований является основной функцией процесса сбора информации:

- *требование руководства по предоставлению особо важной информации* – это требование руководства к подразделениям по предоставлению информации, необходимой для принятия своевременных и правильных решений. Существует два ключевых элемента требований командира: информация о дружественных силах и предоставление информации по приоритетным вопросам.

- *предоставление информации по приоритетным вопросам* является важным разведывательным требованием, необходимым для руководства в целях получения всех сведений о противнике и оперативной обстановке.

- *необходимая информация от дружественных сил* - это информация необходимая руководству для полного понимания позиции и боевой возможности дружественных и содействующих сил.

1-14. *Требования к планированию и оценка процесса сбора информации* включает в себя шесть действий, которые не всегда связаны с деятельностью подчиненных структур. Требования к планированию и оценка процесса сбора информации оказывают содействие группе планирования штаба в ходе проведения объединенных наземных операций.

ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ (MILITARY DECISIONMAKING PROCESS)

1-15. После получения миссии, командиры и штабы начинают осуществлять MDMP. Военный процесс принятия решений является интерактивной

методологией планирования, которая объединяет деятельность командира, сотрудников, подчиненных штаб-квартир и союзников для полного понимания существующей ситуации и миссии; помогает разработать и сравнить варианты действий; выбрать план, который позволит эффективно выполнить миссию.

1-16. Вторым этапом MDMP является анализ миссии. Командиры и штабы анализируют отношения между основной задачей, противником, рельефом местности и погодными условиями, войсками и силами содействия, временными ограничениями, человеческим фактором, что позволяет более глубоко понять:

- Оперативную обстановку, в том числе силы противника и человеческий фактор;
- Желаемый конечный результат вышестоящего руководства;
- Миссию и ее понимание вышестоящим руководством;
- Доступные силы и средства для успешного выполнения миссии и связанных с ними задач.

1-17. OSINT оказывает поддержку группе планирования штаба в процессе MDMP, в результате предоставления предварительной оценки о развитии обстановки на основе сведений из открытых источников. Следует отметить, что IPB (разведывательная подготовка к боевым действиям) является основной частью процесса анализа миссии.

Примечание. Сотрудники военного ведомства (не относящиеся к разведке) также могут проводить мониторинг общедоступной информации для подготовки конкретных прогнозов, документов, брифингов, планов и заказов в целях осуществления поддержки процесса MDMP.

РАЗВЕДЫВАТЕЛЬНАЯ ПОДГОТОВКА К БОЕВЫМ ДЕЙСТВИЯМ (INTELLIGENCE PREPARATION OF THE BATTLEFIELD - IPB)

1-18. Разведывательная подготовка к боевым действиям является систематическим процессом анализа и визуализации угроз, рельефа местности, погодных условий и человеческого фактора в интересующем регионе для определенной задачи.

В результате применения IPB, командиры получают всю необходимую информацию, которые можно выборочно применить и максимально увеличить эффективность работы в критических точках во времени и пространстве.

1-19. Изначально IPB был разработан для поддержки MDMP и порядка действий командира по управлению войсками, но в настоящее время он также применяется в структурах других моделей решения проблем, таких как

проведение «военных игр» и штабных учений. OSINT отвечает разведывательным и информационным требованиям MDMP и играет неотъемлемую роль в процессе разведывательной подготовки к боевым действиям, тем самым поддерживая проведение объединенных наземных операций.

Для эффективной разведывательной подготовки к боевым действиям, подразделение, ведущее разведку в открытых источниках, предоставляет информацию о:

- населении;
- пропаганде;
- тыловом обеспечении;
- оперативной обстановке.

1-20. В основном, процесс разведывательной подготовки к боевым действиям используется командирами и штабами в качестве инструмента анализа конкретных данных для полного понимания региона, в которых планируется проведение операции. До проведения операции необходимо осуществить проверку объединенных и вышестоящих баз данных США и союзников на вопрос наличия интересующей информации.

В ходе проведения операции, требования к разведке и добываемым сведениям определяются в результате развития обстановки. Публично доступная информация из открытых источников может быть использована для соответствия разведывательным и информационным требованиям и оказанию поддержки всем видам разведки.

ГЛАВА 2

ПЛАНИРОВАНИЕ И ПОДГОТОВКА РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ

При проведении операций, общедоступная информация и открытые источники напрямую или косвенно составляют основу всех видов разведки. Эта основа образуется за счет всех компонентов СМИ, которые обеспечивают осведомленность о международных событиях и их восприятия жителями других стран.

Постоянная осведомленность позволяет командирам разработать план. При этом процесс планирования начинается после определения разведывательных и

информационных требований, а также разработки способов их достижения. Эффективное планирование и подготовка миссии OSINT проводится при формировании, обучении частей и соединений Сухопутных войск, что позволяет облегчить их переход к ведению боевых действий.

РАЗДЕЛ I – ПЛАНИРОВАНИЕ ДЕЯТЕЛЬНОСТИ OSINT

2-1. *План* - это этап разведывательного процесса, состоящий из мероприятий, которые определяют требования к информации и разрабатывают способы соответствия этим требованиям и видением конечного результата вышестоящим руководством. Ведение разведки в открытых источниках является основным аспектом степени разведывательной готовности и частью постоянного процесса по сбору информации разведывательными подразделениями, планирование которого начинается до получения официального приказа.

2-2. В центре внимания исследований OSINT оказываются вопросы, определенные руководством до развертывания военного контингента и начала военной операции. Постоянный и активный мониторинг открытых источников с использованием основных и передовых методов поиска в Интернете играет важную роль для лучшего понимания среды проведения операции. Основные сведения, размещенные в открытых источниках, повышают степень боевой готовности войск и позволяют вышестоящему руководству эффективно осуществлять процессы планирования.

При планировании операции, исследования в открытых источниках дают представление о том, как нетрадиционные вооруженные формирования, иностранные вооруженные силы, террористические организаций действуют в подобных регионах, и позволяет в дальнейшем использовать их опыт. До начала развертывания войск, подразделения, занимающиеся разведкой в открытых источниках, могут предоставлять ответы на разведывательные и информационные запросы (смотрите приложение E).

2-3. После получения подразделением миссии, основным направлением деятельности подразделений OSINT является сбор данных из открытых источников о регионе проведения операции. При планировании единой наземной операции, подразделения OSINT предоставляют ситуационные изменения обстановки. Эффективное изучение и планирование позволяет командирам получать своевременные, актуальные и точные разведданные и информацию, которые необходимы для успешного выполнения поставленных задач.

Процессы принятия решений и разведывательная подготовка к боевым

действиям формируют план действий подразделений, ведущих разведку в открытых источниках. OSINT входит в состав процесса планирования с помощью четырех этапов разведывательной подготовки к боевым действиям:

- Определение региона проведения операции;
- Определение влияния окружающей среды на проведение операции;
- Оценка угроз;
- Определение сценариев развития угроз.

ОПРЕДЕЛЕНИЕ ОПЕРАЦИОННОЙ СРЕДЫ

2-4. При анализе условий, различных обстоятельств в зоне проведения операции и интересующих регионах, сотрудники разведки изучают все характеристики оперативной обстановки. Информация из открытых источников может использоваться для определения значительных отличий, от уже имеющихся данных, путем анализа рельефа местности, погодных условий, угроз и человеческих факторов. В конечном этапе процесса разведывательной подготовки к боевым действиям, общедоступная информация и открытые источники могут быть использованы для анализа зоны проведения операции и интересующих регионов.

ОПИСАНИЕ ВЛИЯНИЯ ВНЕШНИХ ФАКТОРОВ НА ПРОВЕДЕНИЕ ОПЕРАЦИИ

2-5. При анализе воздействия внешних факторов на проведение операции, публично доступная информация из открытых источников может быть использована для составления справок о:

- физической среде (наземных, воздушных, морских, космических и информационных областей);
- погодных условиях;
- человеческом факторе;
- имеющихся угрозах.

2-6. Описание воздействия внешних факторов на проведение операции объединяет возможные пути влияния рельефа, погодных условий и человеческого фактора в единый материал, отвечающий требованиям командира. В конце второго этапа разведывательной подготовки к боевым действиям, общедоступная информация и открытые источники могут быть использованы для эффективного информирования командира о возможных

сценариях развития угроз и предоставления соответствующих прогнозов.

ОЦЕНКА УГРОЗ

2-7. Третий этап процесса разведывательной подготовки к боевым действиям является оценка каждого из основных угроз в зоне проведения операции. Если сотрудники не в состоянии определить все существующие угрозы (основные участвующие группы, их боевые возможности, используемое оборудование, степень боевой подготовки, тактику, методы и процедуры, а также их историю) сотрудники будут лишены разведывательных сведений, необходимых для планирования. В конце третьего этапа разведывательной подготовки к боевым действиям общедоступная информация из открытых источников может предоставить основную часть разведанных, необходимых для определения характеристик существующих и ожидаемых угроз.

ОПРЕДЕЛЕНИЕ СЦЕНАРИЕВ РАЗВИТИЯ УГРОЗ

2-8. Четвертый этап процесса разведывательной подготовки к боевым действиям состоит из: выявления, изучения и определения возможных сценариев развития угроз, которые могут повлиять на успешное выполнение боевой операции. Конечным результатом четвертого этапа является составление возможного порядка действий командира вражеских сил, и определение тех методов и способов действий, которые выбрал противник. Вследствие этого общедоступная информация из открытых источников может быть использована для определения дальнейших шагов командования вражеских сил.

РАЗДЕЛ II – ПОДГОТОВКА ПРОЦЕССА ВЕДЕНИЯ РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ

2-9. В результате чрезмерного доверия к секретным сведениям, военнослужащие часто оказывались неосведомленными о существующей оперативной обстановке и плохо подготовленными к использованию огромного объема несекретной информации из общедоступных информационных и открытых источников. Следующая цитата говорит за себя:

Разведка в открытых источниках была довольно новой для нас и как только мы поняли этот термин, мы назначили аналитика радиоэлектронной разведки ответственным за сбор информации из открытых источников.

После одного случая разведка в открытых источниках показала свою эффективность. Террористы провели три успешные атаки на военные самолеты дружественных сил в определенном регионе. Мы не смогли понять, как это произошло и не смогли ответить на «5 вопросов» (кто, что, когда,

где, почему). Но аналитик OSINT нашел видео сбитых самолетов в сети Интернет, что помогло нам определить маршруты передвижения боевиков при проведении атаки. Потом мы установили «беспилотную зону» и успешно блокировали район в зоне проведения операции.

(Аналитик центра сбора разведывательной информации из всех видов источников, военнослужащий боевой авиационной бригады в операции по освобождению Ирака в 2008-2009 гг.)

ВЕДЕНИЕ РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ

2-10. При подготовке к проведению OSINT следует уделить внимание следующим областям:

- Общественные выступления (форумы, конференции);
- Общедоступные документы;
- Телевизионные трансляции;
- Интернет-ресурсы (вебсайты).

Общественные выступления (форумы, конференции)

2-11. Получение информации в ходе общественных выступлений требует точного координирования и синхронизации разведки в открытых источниках с планом сбора информации. При этом необходимо следовать законодательной основе, запрещающей несанкционированный сбор информации в разведывательных целях. (Для дополнительной информации см. приложение А).

2-12. До осуществления разведки в открытых источниках в ходе общественных выступлений необходимо:

- сотрудники разведки должны координировать свои действия с персоналом штаба: заместителем НШ или офицером штаба агентурной разведки и контрразведки (G-2X/S-2X), заместителем НШ или офицером штаба по вопросам информационного воздействия (G-7/S-7), заместителем НШ или офицером штаба по вопросам связи с гражданской администрацией и населением (G-9/S-9), офицером по связям с общественностью (PAO), начальником военно-юридической службы (SJA).

- назначить дополнительные подразделения службы безопасности и требования к техническому обеспечению;

- определить процедуры по установке и демонтажу аудио и видео аппаратуры.

2-13. При сборе информации в ходе общественных выступлений, оперативный приказ(OPORD), тактические приемы, методы и способы (ТТР), установленный порядок действий подразделения (SOPs) описывают детальный план работы подразделения по запросу и распределению финансовых средств с целью закупки цифровой и звукозаписывающей аппаратуры, компьютерного оборудования с программным обеспечением для воспроизведения и хранения видео данных.

ОБЩЕДОСТУПНЫЕ ДОКУМЕНТЫ

2-14. Каждое подразделение осуществляют задания по сбору документов в своих зонах ответственности. Собранные документы тщательно анализируются и распространяются по всему разведывательному сообществу. Перед выполнением любых операции по ведению разведки в открытых источниках необходимо:

- Координировать процесс сбора документов, обработки и анализа информации на всех уровнях военной иерархии;
- Определить порядок развертывания, обслуживания, восстановления и передачи мультимедийного оборудования и средств связи для печатной, аналоговой и цифровой обработки;
- Определить академические и коммерческие информационные услуги, которые уже доступны для сбора, обработки и анализа информации из открытых источников.

2-15. Оперативный приказ, стандартные операционные процедуры подразделения и тактические приемы, методы и способы при ведении боевых действий должны описывать механизм запроса, управления и распределения финансовых средств для:

- услуг сбора и обработки документов;
- закупки книг, словарей, изображений, карт, газет, журналов, аудио и видео записей, компьютерной техники, цифровых камер и сканирующего оборудования;
- подписки на получение газет, журналов и других материалов.

2-16. Для дополнительной информации об использовании общедоступных документах, см. ТС 2-91.8.

ОБЩЕСТВЕННОЕ ТЕЛЕ- И РАДИОВЕЩАНИЕ

2-17. Директор национальной разведки Центра открытых источников (DNI OSC) занимается сбором, обработкой, а также сообщает о международных и региональных вещательных мероприятиях. Это позволяет оперативным подразделениям получать и обрабатывать информацию из местного вещания, интересующую вышестоящее командование. До ведения разведывательных мероприятий в общественном вещании необходимо:

- Координировать процесс сбора, обработки и подготовки отчетов информации из общественного вещания с Центром открытых источников;
- Определить процедуры развертывания, обслуживания, восстановления и передачи радио- и телевизионных цифровых устройств для хранения и обработки содержания, а также систем связи;
- Определить Интернет-источники для сбора и обработки информации из конкретных теле- и радиотрансляций.

2-18. Оперативный приказ, стандартные операционные процедуры подразделения и тактические приемы, методы и способы при ведении боевых действий должны описывать механизм запроса, управления и распределения финансовых средств для закупки антенн и компьютерного оборудования, услуг машинного перевода или программного обеспечения, а также подписки к региональным и международным спутниковым провайдерам радио- и телевещания.

ИНТЕРНЕТ ВЕБ-САЙТЫ

2-19. Собранная, обработанная и правильно предоставленная информация из Интернета оказывает поддержку при проведении объединенных наземных операций. До использования техники ведения разведки в Интернете необходимо:

- Скоординировать и организовать процесс сбора, обработки и анализа информации из Интернета во всех эшелонах подразделения;
- Определить процедуры развертывания, обслуживания, восстановления и передачи компьютеров и связанных с ними систем связи и хранения данных;
- Координировать действия с заместителем начальника или офицером штаба связи (G-6/S-6) для получения доступа к сети INTELINK-U или утвержденных коммерческих Интернет-провайдеров, которые поддерживают

требования по сбору, обработке, хранению и распределению информации из открытых источников;

- Координировать действия с заместителем начальника или офицером штаба связи (G-6/S-6) с целью разработки перечня разрешенных внутренних и иностранных Интернет веб-сайтов для служебного пользования, исследований с использованием открытых источников, а также иностранных веб-сайтов, доступных только ограниченному (уполномоченному) персоналу, ведущему разведку в открытых источниках;

- Определить академические и коммерческие открытые информационные услуги, которые доступны для сбора, обработки и анализа информации.

2-20. Оперативный приказ, стандартные операционные процедуры подразделения и тактические приемы, методы и способы при ведении боевых действий должны описывать механизм работы подразделения, осуществляющего научно-исследовательские операции в сети Интернет. В соответствии с вышеуказанными процедурами, подразделение направляет запросы, распределяет и управляет средствами для приобретения оцифрованных документов, геопространственной информации, компьютерного оборудования и программного обеспечения, а также любых подписок на академические и коммерческие онлайн базы данных, газет, журналов и ссылок.

ПОДГОТОВКА К ПРОВЕДЕНИЮ OSINT

2-21. Подготовка к ведению разведки в открытых источниках также включает:

- Создание структуры OSINT;
- Классификация приоритетов задач и запросов;
- Персонал по подготовке задач;
- Оперативные кадры;
- Оценку проведенных операций.

Создание структуры OSINT

2-22. OSINT способствует формированию структуры разведки. Создание структуры разведки включает в себя сложные технические вопросы, состоящие из следующих элементов: технические средства, информационный поток, программное обеспечение, средства связи, обеспечение безопасности связи, доступ к базе данных, засекречивание сетей, технические специалисты, офицеры

связи, подготовка разведывательной деятельности и финансирование.

Четко разработанная и сформированная структуры разведывательного органа помогает компенсировать и смягчить структурные и организационные недостатки, а также нехватку личного состава. Эффективная структура создает все необходимые условия для наилучшего понимания руководством угроз, рельефа местности и погодных условий и человеческого фактора в зоне проведения операции.

Установлено, что такие элементы структуры OSINT, как постоянный поток информации, технические средства, программное обеспечение, безопасность средств коммуникации и базы данных состоят из:

- **Обеспечения доступности разведывательных данных.** *Доступность разведанных* является процессом, при котором разведывательные организации активно и быстро получают доступ к разведанным и необходимую информационную поддержку, осуществляют прямое сотрудничество и обмен информацией с другими подразделениями и учреждениями как внутри, так и за пределами района проведения операций, не ограниченных географической близостью, эшелонами или командами.

- **Разработки и ведения автоматизированной сети разведки.** Главной задачей является предоставление информационных систем, которые обеспечивают связь между сотрудниками, подразделениями, соединениями, агентствами и государствами-союзниками для ведения разведки, совместного анализа и обработки, распространения материалов и создания условий доступности разведывательных данных.

В настоящее время используются существующие автоматизированные информационные системы, а в случае необходимости оперативно создаются специфические сети.

- **Создания и поддержания доступа.** Эта задача влечет за собой установление, обеспечение и поддержание доступа к секретным и несекретным программам, базам данных, сетям, системам и другим Интернет ресурсам для войск союзных государств, объединенных сил, национальных агентств и международных организаций.

- **Создания и ведения баз данных.** Эта задача предполагает создание и поддержание несекретных и секретных баз данных. База данных необходима для создания среды, обеспечивающей взаимодействие и совместную работу войск, объединенных сил, государственных агентств и международных организаций.

Создание и ведение базы данных способствует быстрому анализу, подготовке отчетов, обработке, распространению, ведению длительных боевых действий.

Оперативные и технические базы данных открытых источников

2-23. Для ведения разведки в открытых источниках требуется доступ к базам данных и возможностям сети Интернет в целях облегчения, эффективной обработки, хранения, поиска и обмена открытой информацией. Эти базы данных размещены в локальных вычислительных сетях (ЛВС), «World Wide Web» (WWW), и «Deep Web» (см. Приложение С для получения дополнительной информации).

Для оказания поддержки объединенным наземным операциям, сотрудники OSINT используют проанализированную информацию из открытых источников и пополняют следующие информационные базы данных:

- **База данных с оперативной информацией** обеспечивает взаимосвязь между приказами и запросами, показывает статус процесса сбора материалов, обработки, и содержит статистические данные (графики, таблицы);

- **База данных с технической информацией** поддерживает операций по сбору информации и состоит из необработанных текстовых, аудио- и видео материалов, переводов и записей (стенограмм).

Требования к материально-техническому обеспечению процесса сбора информации из открытых источников – система управления (OSCAR-MS)

2-24. Основные требования к управлению оперативной и технической базами данных указаны в материально-техническом обеспечении процесса сбора из открытых источников – система управления (OSCAR-MS). OSCAR-MS представляет собой веб-сервис, спонсируемый Управлением первого помощника заместителя Директора национальной разведки открытых источников (ADDNI/OS), который определяет для Национального предприятия открытых источников (National Open Source Enterprise -NOSE) требования по сбору данных из открытых источников.

Система управления OSCAR-MS объединяет работу сотрудников занимающихся разведкой в открытых источниках и сотрудников, использующих собранные материалы, начиная от уровня разведывательного сообщества до бригадных тактических групп (ВСТ).

Сотрудники бригадных тактических групп получают доступ к системе управления OSCAR-MS с помощью Секретной сети «SECRET Internet Protocol Router Network» (SIPRNET), с целью направления запросов по необходимой

информации в Департамент службы информационной разведки Сухопутных войск США (DA IIS).

Основной целью системы управления OSCAR-MS является автоматизация и рационализация специальных требований по сбору информации из открытых источников с помощью:

- Определения необходимых исходных параметров для полного понимания требований к подразделениям, ведущих разведку в открытых источниках;

- Разрешения электронной классификации и учета, запрошенных и обработанных материалов из открытых источников, в целях облегчения процесса поиска необходимой информации в Библиотеке национальной разведки;

- Обеспечения подчиненных подразделений всеми необходимыми административными данными (управление зонами ответственности подразделениями, местные таблицы данных и местные форматы);

- Разрешения простых методов автозаполнения базы данных;

- Использования полного написания слов, вместо сокращений, компьютерных программ и других ярлыков;

- Разрешения взаимосвязи между требованиями, материалами и оценками;

- Организации объединения пользователей открытых источников для сотрудничества между агентствами;

- Сокращения дублирования требований.

2-25. Для получения более детальной информации о системе управления OSCAR-MS или для получения требований к OSINT, необходимо обратиться в Командование разведки и безопасности Сухопутных войск США при Департаменте службы информационной разведки.

Определение степени важности задач и запросов

2-26. Помощник начальника штаба /офицер штаба по разведке и помощник начальника штаба/офицер оперативного отдела штаба (G-2/S-2 и G-3/S-3) для завершения плана сбора разведывательных данных используют инструкции руководства и основные требования к ведению разведки. План используется для определения задач подчиненным подразделениям или направления запросов во взаимодействующие разведывательные органы в целях достижения желаемых результатов в процессе сбора информации в открытых источниках. Данные задачи, входя в состав плана по сбору информации, определяют алгоритм работы подразделений при:

-направлении запросов в объединенные, межведомственные, межправительственные и межгосударственные разведывательные организации по сбору и обработке необходимой информации, в целях получения информационной поддержки;

-формировании задач и развертывании работы действующих, прикрепленных сил и средств, занимающихся вопросами сбора, обработки и подготовки материалов;

-использовании дистанционных, сравнительных и распределенных методов сбора, обработки и производства материалов;

-осуществлении запроса и управлении работой американских и неамериканских (*не являются гражданином*) лингвистов по степени необходимости, опыту ведения конкретных боевых операции, уровня доступа к секретной информации, категорий и требований к знаниям языка и диалекта;

2-27. При разработке задач по сбору информации для подчиненных подразделений помощник начальника или офицер штаба по разведке и помощник начальника штаба или офицер оперативного отдела штаба используют задачи и цели, построенные для формирования структуры задач и определения следующих вопросов:

- исполнитель;
- суть;
- временные параметры;
- район проведения.

Силы и средства организации задания

2-28. За исключением азиатского отдела исследований (ASD), который совместно с правительством Японии оказывает логистическую поддержку Тихоокеанскому командованию США (USPACOM), Сухопутные войска не имеют всей необходимой поддержки для сотрудников и подразделений OSINT при подготовке процесса проведения разведки в открытых источниках.

Развертываемые силы и средства

2-29. Развертывание общедоступных сил и средств:

- поддерживает схемы передвижения войск;
- поддерживает цели командира;
- соответствует стандартам ведения боевых действий подразделениями.

2-30. Силы и средства необходимо развертывать в безопасном местоположении с доступом к сети Интернет, в непосредственной близости от

ресурсов жизнеобеспечения, защиты и коммуникации.

Процесс анализа проведенных операций

2-31. Принципы для анализа операций:

- мониторинг;
- сравнение и отбор поступающих отчетов;
- построение механизма обратной связи с источниками информации (постановка задач, корректировка их деятельности, определение приоритетов);
- информационное обеспечение.

2-32. Для получения полной информации см. пункт 2-67.

РАЗДЕЛ III – ФАКТОРЫ, ВЛИЯЮЩИЕ НА ПРОЦЕСС ПЛАНИРОВАНИЯ И ПОДГОТОВКИ

2-33. Факторы, влияющие на процесс планирования и подготовки ведения разведки в открытых источниках, включают:

- надежность открытого источника;
- достоверность содержания информации;
- соответствие;
- мероприятия по обеспечению безопасности (OPSEC);
- гриф секретности;
- координация;
- дезинформация;
- авторское право и интеллектуальная собственность;
- лингвистические требования;
- автоматизированная система перевода иностранного языка;

НАДЕЖНОСТЬ ОТКРЫТЫХ ИСТОЧНИКОВ

2-34. Виды источников, используемые для оценки информации:

- основной источник;
- дополнительный источник.

2-35. **Основным источником** является документ или физический объект, содержащий информацию, которая была написана или создана в результате исследований и анализа. Данные источники являются непосредственными свидетелями того или иного события и содержат «инсайдерскую информацию». Основные источники:

- классифицируются по содержанию;
- являются государственным или частным;
- упоминаются в качестве первоисточника или доказательства;

- как правило, такая информация является фрагментарной, неоднозначной и сложной для анализа.

2-36. Некоторые виды основных источников:

- оригиналы документов (выписки и переводы), дневники, конституций, научные журналы, выступления, рукописи, письма, интервью, новостные и видео кадры, автобиографий и официальные отчеты;
- творческие работы: поэзия, драматургия, романы, музыка и искусство;
- реликвии и артефакты: керамика, мебель, одежда, артефакты и исторические здания;
- персональные рассказы и воспоминания;
- человек-первоисточник.

2-37. **Дополнительные источники** интерпретируют, анализируют, цитируют и ссылаются на основной источник (первоисточник). Дополнительные источники могут содержать картинки, цитаты и графику из основных источников. Некоторые виды дополнительных источников включают:

- историй;
- учебники;
- критики;
- статьи из журналов;
- энциклопедий;
- комментариев.

***Примечание:** Основные и дополнительные источники часто трудно различить, так как они носят субъективный характер. Основные источники не всегда являются достоверными и более надежными, чем дополнительные источники. В не зависимости от источника информации для сотрудников разведки в открытых источниках важно оценить и проанализировать достоверность и наличие дезинформирующих элементов.*

2-38. Как указано в таблице 2-1, степень надежности открытых источников дифференцируется от **A** (надежный) до **F** (надежность не установлена). Источник, который впервые используется в проведении OSINT, автоматически получает степень надежности **F**. Присуждение степени **F** не означает, что источник является ненадежным, но означает, что сотрудники OSINT ранее не использовали данный источник.

Надежный	Нет сомнения в подлинности, достоверности и
-----------------	--

	компетентности источника; предоставляет достоверную информацию на постоянной основе
Обычно надежный	Незначительные сомнения в подлинности, достоверности и компетентности источника; большую часть времени предоставляет достоверную информацию
Редко надежный	Сомнение в подлинности, достоверности и компетентности источника, однако в прошлом предоставляло надежную информацию
Обычно не надежный	Значительные сомнения в подлинности, достоверности и компетентности источника, однако в прошлом предоставляло надежную информацию
Ненадежный	Недостаточная подлинность, достоверность и компетентность источника; в прошлом предоставляло недостоверную информацию
Надежность не установлена	Отсутствуют основания для оценки надежности источника

Таблица 2-1. Степени надежности источников

ДОСТОВЕРНОСТЬ СОДЕРЖАНИЯ ИНФОРМАЦИИ В ОТКРЫТЫХ ИСТОЧНИКАХ

2-39. Как указано в таблице 2-2, подобно степеням надежности источников, показатели достоверности информации варьируются от **одного** (достоверность подтверждена) до **восьми** (достоверность не установлена). Следует отметить, что если источник используется впервые, то ему присуждается восьмая степень достоверности. Присуждение степени восемь не означает, что источник является недостоверным, но означает, что сотрудники OSINT не имеют средств проверить достоверность.

Подтвержденный	Подтверждается другими независимыми источниками; имеет логическую структуру; согласуется с другой информацией по данному вопросу
Вероятно точная	Не подтверждается другими независимыми

информация	источниками; имеет логическую структуру; согласуется с другой информацией по данному вопросу
Возможно точная информация	Не подтверждается; имеет разумную логическую структуру; согласуется другими некоторыми информациями по данному вопросу
Сомнительно точная информация	Не подтверждается; возможный, но не имеет логической структуры; не согласуется другими информациями по данному вопросу
Неправдоподобная информация	Не подтверждается; не имеет логической структуры; противоречит другим информациями по данному вопросу
Дезинформация	Ненамеренно ложная; не имеет логической структуры; противоречит другим информациям по данному вопросу; дезинформация подтверждена независимыми источниками
Обман	Заведомо ложная; противоречит другим информациям по данному вопросу; обман подтвержден независимыми источниками
Не может быть определен	Не существует основы для оценки достоверности информации

Таблица 2-2. Степень достоверности открытых источников

СООТВЕТСТВИЕ

2-40. В соответствии с EO 12333, DOD 5240,1-R и AR 381-10, процедура №2, Сухопутные войска могут вести разведывательную деятельность по сбору необходимой информации из открытых источников о гражданах США только тогда, когда это необходимо для выполнения определенных функций.

(Для получения дополнительной информации о контроле над деятельностью разведки см. приложение А).

МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

2-41. Ведение разведки в открытых источниках непреднамеренно может раскрыть показатели настоящих и будущих военных операций США. Информация, предоставленная широкой общественности, может выявить

существование, а иногда и подробности секретной или конфиденциальной информации, которая может быть использована для нейтрализации или проведения военных операций. Разведывательные организации должны определить уровень контактов с открытыми источниками, а также сбор или приобретение техники, которые могут повлиять на проведение наземных операций.

ГРИФ СЕКРЕТНОСТИ

2-42. AR 380-5 гласит, что составители разведывательных материалов «должны быть осторожны при определении грифа секретности. Присуждение чрезмерно высокой степени секретности лишает доступа военнослужащих ко многим полезным материалам». Это также является предупреждением для сотрудников OSINT, занимающихся обеспечением безопасности, которые могут поставить под угрозу осуществление процесса распределения несекретной информации.

Примеры несекретной информации, которая была чрезмерно засекречена:

- информация, находящаяся на страницах зарубежной газеты;
- выступление иностранного должностного лица на международной конференции.

2-43. AR 380-5 указывает, что военнослужащие не будут присуждать гриф секретности или другие маркировки безопасности для статьи или части статьи, которая появилась в газете, журнале или других открытых источниках. Окончательный анализ, исследования, документы, материалы OSINT могут потребовать дополнительных ограничений, и считаться контролируемой несекретной или чувствительной, но несекретной информацией.

КООРДИНАЦИЯ

2-44. Во время планирования, помощник начальника штаба или офицер штаба по разведке и помощник начальника штаба или офицер оперативного отдела штаба должны убедиться, что цели и задачи разведки в открытых источниках синхронизируются со схемой передвижения войск. Сбор информации из открытых источников может поставить под угрозу деятельность других видов разведки и тактических подразделений. Несинхронизированный сбор информации из открытых источников, также может привести к неправильному использованию сил и средств, что отрицательно повлияет на способность

неразведываемых организаций (военной полиции и организаций по делам общественности) выполнять поставленные задачи. Открытые контакты с открытым источником неразведываемых организаций может поставить под угрозу цели и задачи процесса ведения разведки в открытых источниках и привести к потере разведанных.

ДЕЗИНФОРМАЦИЯ

2-45. В процессе ведения разведки в открытых источниках необходимо учитывать присутствие дезинформации. Сотрудники подразделения, ведущего разведку в открытых источниках, обычно не получают информацию путем прямого наблюдения за деятельностью и условиями места проведения военной операции. Они опираются в основном на вторичные источники. Такие вторичные источники, как правительственные пресс-службы, новостные коммерческие организаций, пресс-секретари и неправительственные организаций, могут преднамеренно или непреднамеренно добавлять, удалять, изменять или иным образом фильтровать информацию, поступающую для широкой общественности. Эти источники могут также передать одно сообщение на английском языке с целью оказания влияния на США или международные сообщество и другое сообщение с другим смыслом не на английском языке для оказания влияния на местное население.

Важно знать историю открытых источников (информагентств) и определить цель информации для того, чтобы различить цели, фактическую информацию, выявить предвзятость, обман, а также определить попытки оказания влияния на читателей и на ход военной операции.

АВТОРСКОЕ ПРАВО И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

2-46. Авторское право является одной из форм защиты, опубликованных и неопубликованных работ, предусмотренных главой 17 Кодекса США, что определяет авторов «оригинальных работ авторов», в том числе литературных, драматических, музыкальных и художественных произведений.

Интеллектуальной собственностью считается любое творение ума и включает, но не ограничивается:

- музыкальные произведения и композиций;
- художественное выступление;
- открытия;
- изобретения;
- слова или фразы;

- символы и рисунки.

22-47. Нарушение прав, предусмотренных законом об авторских правах, является незаконным. Одним из основных ограничений является доктрина правомерного использования, законодательная основа которой описана в статье 107 «Закона об авторском праве» 1976 г.

По данным Управления охраны авторских прав США, «правомерное использование», защищенных авторскими правами работ в таких целях, как использование в критике, комментариях, новостях, исследованиях, обучении в школах и университетах не является нарушением авторских прав. Четыре фактора, определяющие правомерное использование:

- цель и характер использования;
- свойства, используемых авторских работ;
- количество и часть авторской работы, которая используется;
- воздействие использования авторских работ на потенциальный рынок или ценность этих работ.

2-48. AR 27-60 описывает основные процедуры необходимые для приобретения, защиты, передачи, использования патентов, авторских прав, товарных знаков и интеллектуальной собственности. Политика Сухопутных войск США признает права владельцев авторских прав в соответствии со своей миссией и обязательствами во всем мире. Сотрудники подразделения OSINT не будут использовать и распространять охраняемые авторским правом работы без разрешения владельца авторских прав, кроме тех случаев, когда такое использование разрешено в соответствии с законодательством США об авторском праве. Сотрудникам OSINT необходимо направлять запрос в юридическую службу штаба (SJA) в целях одобрения или отказа от уведомления правообладателя, что может быть необходимо для обеспечения безопасности операции (OPSEC).

ЛИНГВИСТИЧЕСКИЕ ТРЕБОВАНИЯ

2-49. При проведении разведки в открытых источниках способность собирать и анализировать материалы на иностранном языке является важным элементом.

Эффективное использование и привлечение лингвистов, как гражданских, так и военных, облегчает эту деятельность. Области, в которых критически важно знание иностранного языка и высокая квалификация:

- *Транскрипция*. При прослушивании и записи является очень важным знанием

языка в целях точной записи стенограммы. В таких случаях, когда знание английского языка сотрудников OSINT недостаточны для официального или прямого перевода аудио- или видео материалов на английский язык, стенограмма является чрезвычайно важным.

- *Перевод* (письменный). Знание двух иностранных языков является необходимым условием для осуществления переводов. Лингвисты должны уметь:

- читать и понимать исходный язык;
- хорошо писать на английском языке;

- при переводе выбирать эквивалентные выражения на английском языке, которые полностью передают и наилучшим образом соответствует смыслу иностранного слова;

- *Интерпретация* (устный перевод). Знание двух иностранных языков является необходимым условием для интерпретации. Лингвисты должны уметь:

- слышать и понимать исходный язык;
- понятно разговаривать на английском языке;

- выбирать эквивалентные выражения на английском языке, которые полностью передают и наилучшим образом соответствует смыслу иностранного слова;

Примечание. Интерпретация является специальным навыком, которому обучены не все лингвисты.

2-50. В целях эффективного планирования и использования лингвистов, командиры и офицеры штаба должны понимать систему оценки лингвистических знаний военнослужащих. Оценка и переоценка знаний лингвиста подробно описана в AP 11-6, глава 5. Тестирование языка является обязательной процедурой для всех военнослужащих, прошедших обучение иностранного языка, в зависимости от языка военно-профессиональной специальности (MOS) или профессионального кода армии (AOC). Другие военнослужащие, знающие иностранные языки могут пройти соответствующее тестирование и работать в качестве лингвиста.

2-51. Сухопутные войска для определения уровня владения иностранным языком используют тест по проверке уровня языковой подготовки военнослужащих «Defense Language Proficiency Test» (DLPT). DLPT определяет только языковые возможности военнослужащих, и не является окончательной оценкой способности человека оказывать лингвистическую поддержку.

2-52. Армия использует систему описания Межведомственного языкового

круглого стола (ILR), которая определяет уровень знания, навыки общения, аудирования, чтения и письма на иностранном языке. Подробные описания этих уровней можно найти на сайте <http://www.govtilr.org>. Обозначение уровень-плюс, как показано символом «+», используется, когда знания лингвиста выше базового уровня, но еще недостаточны для перехода на следующий уровень. Существуют шесть базовых уровней:

- уровень 0 (без навыков). Военнослужащий не обладает функциональными способностями. Уровень 0 + является минимальным стандартом для спецназа и указывает на способность запоминать иностранные слова.

- уровень 1 (элементарное владение). Военнослужащий имеет ограниченные знания иностранного языка, которые соответствуют элементарным требованиям.

- уровень 2 (ограниченное владение). Лингвист достаточно квалифицирован, соответствует обычным требованиям иностранного языка и работы.

- уровень 3 (общая профессиональная квалификация). Лингвист на практическом, социальном и профессиональном уровне способен выполнять общие, технические, формальные и неформальные задачи на иностранном языке.

- уровень 4 (продвинутая профессиональная квалификация). Лингвист способен выполнить любые задачи свободно и точно.

- уровень 5 (родной язык). Лингвист владеет языком эквивалентно четко и хорошо, как и носитель и отражает культурный уровень страны, где иностранный язык является родным.

2-53. До определения базового уровня, определяется уровень четырех языковых навыков: аудирования, чтения, разговорной и письменной способностей. DLPT оценивает только уровень способностей чтения и аудирования (например, 2 +/3 или 3/1+). В настоящее время данные тесты не оценивают лингвистов выше третьего профессионального уровня. В Сухопутных войсках второй уровень является стандартом, а военнослужащий, обладающий этим уровнем, считается квалифицированным лингвистом. Собеседование помогает оценить умение общаться на иностранном языке, и может быть использовано для оценки слуховых (аудиоальных) способностей восприятия иностранной речи. С помощью собеседования можно оценивать лингвистов до пятого уровня.

2-54. При анализе неанглийских открытых источников информации

Исследовательский Центр Виктора Воксанаева
Бюллетень OSINT № 33 (сентябрь – октябрь 2013 г.)

гражданскими переводчиками, наряду с языковыми навыками и беглостью речи, сотрудники OSINT должны учитывать предубеждения и культурные традиции этих переводчиков. При планировании использования лингвистов, командиры должны определить требования по следующим категориям выбор лингвистов:

- категория I. Переводчики должны иметь, по крайней мере, передовые профессиональные знания необходимого иностранного языка (4 уровень согласно системе ILR) и общего рабочего английского языка (ILR 2 +). Они могут быть наняты из или вне области проведения военной операции. Они не требуют допуска к секретным сведениям.

- категория II. Лингвисты являются гражданами США, с разрешения соответствующих служб безопасности правительства США получают доступ к секретной информации и работе. Они должны, по крайней мере, обладать передовыми профессиональными знаниями необходимого языка (ILR 4) и общего рабочего английского языка (ILR 2 +).

- категория III. Лингвисты являются гражданами США. С разрешения соответствующих спецслужб безопасности правительства США получают доступ к работе с совершенно секретной/секретной информацией с особым режимом хранения. Они должны обладать минимум третьим уровнем (ILR 3) знаний английского и иностранного языков.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПЕРЕВОДА ИНОСТРАННЫХ ЯЗЫКОВ (MFLT)

2-55. Процесс подготовки (*обучение и приобретение опыта*) надежных и опытных лингвистов требует много времени, что приводит к нехватке лингвистов. Для заполнения вакансий и соответствия языковым требованиям в ВС США используется автоматизированная система перевода иностранного языка MFLT. При использовании данной системы должным образом, повышаются переводческие возможности в целях поддержания единой наземной операции.

2-56. MFLT обладает программным обеспечением способным переводить любые материалы средств массовой информации и интернет материалы на английский язык. Обладает ограниченными возможностями синхронного перевода (speech-to-speech S2S).

Мониторинг зарубежных информагентств

2-57. Такие системы мониторинга информагентств, как система мониторинга трансляции (BBN BMS) создают непрерывный архив с возможностью поиска международных телевизионных передач. Эти системы автоматически

записывают поток аудио материалов в реальном времени и переводят ее на английский язык. Запись и перевод синхронизированы с видео материалом, что создает огромные возможности для эффективного поиска и точного воспроизведения первоначального видео на основе его содержания речи. С помощью этой системы, аналитики разведывательных организации могут быстро и эффективно проверить огромное количество новостей на иностранных языках.

2-58. Эти системы позволяют в режиме реального времени записывать и переводить телевизионные новости, что помогает сотрудникам быстро сортировать иностранные новости. Система также оповещает, когда содержание новой информации соответствует запросу, установленному в системе, а также в целях осуществления качественных переводов тесно сотрудничает с переводчиками и специалистами в области культуры (регионоведы).

2-59. Интерфейс позволяет пользователям быстро найти содержание конкретного разговора в видеоархиве с помощью запроса по ключевым словам на английском или иностранном языках. Поиск выделяет все результаты, которые показывают уменьшенное изображение стенограммы на языке-оригинале и перевод на английском языке. При нажатии на результат начинается воспроизведение сегмента.

2-60. Пользователи взаимодействуют с системой из любого персонального компьютера (ПК) или ноутбука, подключенных к высокоскоростному Интернету. Для работы с системой необходимо следующее программное обеспечение: Microsoft Internet Explorer и Windows Media Player.

2-61. Система мониторинга трансляции непрерывно собирает, кодирует, анализирует и сохраняет все потоки видео материалов в режиме реального времени в автоматическом и динамическом кэш-накопителе со сроком на 30 дней. Как только видео начинает воспроизводиться, система показывает произнесенные слова, как в языке-оригинале, так и на английском языке. Расшифровка обогащается, выделяя имена людей, мест и организаций, а также в результате разделения голосов. Пользователи могут перейти в любую точку в кэш-накопителе и начать воспроизведение.

2-62. Пользователи могут извлечь видео сегменты или фотографий для использования в презентациях и совместной работе. Демонстрационные компакт-диски (CD) содержат извлеченные сегменты, которые содержат основные моменты видеозаписей и переводов во время их повторного воспроизведения.

2-63. Система BBN BMS в настоящее время переводит:

- стандартный современный арабский язык;
- китайский;
- испанский язык западного полушария;
- персидский (фарси);
- североамериканский английский язык;
- английский язык Соединенного Королевства;
- французский язык;
- индонезийский;
- хинди;
- урду.

2-64. BBN BMS не требует никакого дополнительного оборудования, установки программного обеспечения, веб-администратора или обслуживания пользователями.

Синхронный перевод (speech-to-speech)

2-65. Сухопутные войска и морская пехота по-прежнему пытаются интегрировать устройства синхронного перевода «COTS S2S» в программу подготовки перед развертыванием военных операций и во время начала ее развертывания. Основное тактическое применение для этих устройств является перевод языка при проведении операции среди населения, не владеющего английским языком.

IV РАЗДЕЛ – КОМПЛЕКТОВАНИЕ ЛИЧНОГО СОСТАВА ПОДРАЗДЕЛЕНИЙ OSINT

2-66. Сотрудниками OSINT могут быть лица, обладающие техническими и культурными знаниями, креативностью, предусмотрительностью, общественной осведомленностью, необходимых для эффективного использования открытых источников. В целях удовлетворения требований операций и задач, сотрудники OSINT назначаются командирами в результате проведения реорганизации сил и средств в соответствии с поставленными задачами за счет штатных средств (сотрудников спецслужб, неразведывательного персонала, контрактников или лингвистов).

ОБЯЗАННОСТИ ПОДРАЗДЕЛЕНИЯ OSINT

2-67. В обязанности подразделения OSINT входят:

- *мониторинг операций*, в целях обеспечения своевременного реагирования на сложившуюся ситуацию и прогнозирования требований к сбору, обработке, предоставлению анализа и синхронизации необходимой информации;

- *сравнение разведданных.* Поступающие разведданные (письменные, устные или графические) должны сравниваться с уже имеющимися секретными сведениями;

- *фильтрация разведывательной информации.* Информация отсеивается в соответствии с требованиями командира и его руководством по предоставлению особо важной информации для того, чтобы неактуальная и ненужная информация вырезалась, а необходимая информация перерабатывалась в работоспособный размер. Процесс отсеивания должен включать элементы своевременности, полноты и актуальности в целях соответствия всем разведывательным требованиям;

- *распространение разведданных и информации.* Информация, соответствующая всем требованиям OSINT, распространяется пользователям в виде готовых к использованию материалов и отчетов;

- *взаимодействие.* Эффективное сотрудничество между подразделениями OSINT, агентурной разведкой (HUMINT) и контрразведкой (CI) улучшает общие усилия по сбору информации посредством ситуационного информирования несекретной информацией руководства этих подразделений, а также позволяет использовать многопрофильный подход для проверки достоверности информации, добытой другой разведывательной организацией.

- *обеспечение обратной связи.* Механизм обратной связи необходим для поддержания осведомленности командиров подразделений и частей о степени достоверности разведданных и требований к предоставляемой информации.

ПОДРАЗДЕЛЕНИЕ OSINT НА УРОВНЕ БРИГАДНО-ТАКТИЧЕСКОЙ ГРУППЫ

2-68. Каждое боевое командование в своем составе может иметь отделение или группу OSINT, ведущих разведку в открытых источниках. При проведении операции на тактическом уровне, командиры создают отделения OSINT из основного состава подразделения разведки, в целях соответствия требованиям разведки.

2-69. Следующая цитата описывает, как распределение сил и средств для выполнения задачи в составе боевой группы (CGS) помогает удовлетворять разведывательные и информационные требования. Это достигается посредством использования незащищенной маршрутизированной сети IP-протокола

(NIPRNET) и различных электронных устройств, таких как AM / FM радио, видеомэгаффона (VCR), DVD-плеера, в целях обеспечения успешного сбора информации бригадной тактической группой в центре тактических операций (ТОС):

С их боевой группой, четырьмя или пятью переводчиками, постоянным потоком радио, телевидения и газет, группа ведения разведки в открытых источниках ежедневно накапливает и анализирует информацию.

В их офисе имеют один телевизор с местными и международными кабелем, один ноутбук, подключенный к NIPRNET, AM / FM радио и ежедневные газеты. Кроме того, команда приобрела видеомэгафон и DVD-плеер для изучения конфискованных аудио и видео материалов пропаганды. Они понимают важность отчетов о местности для успешного завершения военной кампании и провели тщательное исследование всех вопросов местного значения. Перед представлением документа офицеру по разведке бригадной тактической группы и распространением в батальоны или дивизии, их материал был изучен и проанализирован группой, занимающейся анализом собранных материалов.

Командир роты разведки, операция по освобождению Ирака 2004-2005гг.

2-70. Как показано на рисунке 2-1, подразделение, занимающееся разведкой в открытых источниках, в составе бригадной тактической группы состоит из:

- Лидера отделения;
- Менеджер требований;
- Аналитик по изучению ситуации;
- Аналитик по изучению задачи.



Рисунок 2-1. Отделение OSINT в составе бригадной тактической группы

Лидер отделения

2-71. Лидер отделения:

- является основным координатором связи и офицером разведки бригадной тактической группы (ВСТ S-2);
- осуществляет контролирующие и управленческие функции;
- устанавливает приоритетные задачи;
- мониторит поступающие разведывательные данные, необходимые для офицера разведки бригадной тактической группы (ВСТ S-2);
- гарантирует, что все материалы OSINT включены в планирование текущих и будущих операций.

Менеджер требований

2-72. Менеджер требований:

- принимает все необходимые меры, чтобы развитие ситуации и разработка цели поддерживали общие усилия подразделения;
- проверяет наличие сил и средств, необходимых для сбора информации;
- осуществляет контроль над качеством материалов по развитию ситуации и разработке целей.
- контролирует процессы получения, анализа и распространения материалов, собранных из открытых источников.

Аналитик по изучению ситуации

2-73. Аналитик по изучению ситуации:

- в целях обеспечения наиболее точной и общей оперативной обстановки, осуществляет мониторинг общедоступной информации в открытых источниках;
- анализирует информацию и выдает текущие разведывательные данные об оперативной обстановке, противнике, местности и человеческих факторах во время подготовки и проведения операции;
- уточняет полученную информацию об угрозах, цели, боевой эффективности и потенциальных операциях;
- подтверждает или опровергает угрозу развития событий на основе общедоступных показателей;
- в целях лучшего понимания местного населения в районе проведения операции аналитик предоставляет следующую информацию о:

- племенной принадлежности;
- политических убеждениях;

- религиозных догмах;
- основных лидерах;
- группах поддержки;
- источниках дохода.

Аналитик по изучению задачи

2-74. Аналитик по изучению ситуации:

- определяет компоненты, элементы и характеристики конкретных задач;
- определяет человеческие и другие факторы в районе проведения военной операции;
- предоставляет информацию о возможных угрозах и ограничениях посредством ведения разведки в открытых источниках.

Аспекты организации

2-75. При проведении реорганизации сил и средств для формирования отделения OSINT, подразделения должны учитывать:

- командование миссии;
- получение информации;
- сбор и обработку информации;
- предоставление материалов;
- компьютерные системы.

Командование миссии

2-76. Для управления и наблюдения за процессом разведки в открытых источниках необходим подбор квалифицированного руководящего состава, который способен синхронизировать и координировать действия элементов (подразделений), задач и запросов.

Получение информации

2-77. В связи с тем, что обширные объемы информации постоянно доступны в открытых источниках, необходимо создать системы с определенным порядком сбора информации. Данный порядок действий позволит избежать утраты и неправильного использования, полученных сведений, которые могут предоставить важную информацию для выполнения задач руководства. Полученные сведения из открытых источников предоставляются в соответствии со стандартными порядками действий подразделения.

Сбор и обработка информации

2-78. С целью соответствия требования командира по предоставлению особо важной информации (CCIRs), процесс сбора сведений из открытых

источников должен быть правильно интегрирован в общий план по сбору информации. Персоналу по обработке документов (DOCEX), при обработке данных часто требуется получение сведений из открытых источников для чего необходимо получение полного доступа к внутренним и зарубежным базам данных общедоступной информации.

Примечание: Персоналу, принимающему участие в сборе и обработке информации, необходимо уметь разделять сведения на общедоступные и те, которые несут важную ценность для разведывательного органа. Далее, данные сведения должны быть изложены в наглядной форме для утверждения у директора агентства национальной безопасности (DIRNSA). Информация из иностранных открытых источников должна быть собрана и обработана в определенной форме, в другом случае данная информация может потерять свою разведывательную важность.

Предоставление материалов

2-79. Предоставление достоверных и своевременных общедоступных сведений является основой для проведения разведки в открытых источниках. С целью получения, интеграции, оценки, анализа и интерпретации общедоступных сведений необходимо использовать различные методы исследований, основные и передовые интернет-технологий и другие инструменты. Полученные сведения и метаданные хранятся базе данных, доступной соответствующему разведывательному и неразведывательному персоналу.

Компьютерные системы

2-80. Персонал, занимающийся разведкой в открытых источниках, должен использовать программное обеспечение, предназначенное для выполнения соответствующих задач. В список необходимых программ входят «Analyst Notebook», «Portable Document Format (PDF) Maker» и «Text Chart» (текстовые диаграммы).

ГЛАВА 3

СБОР РАЗВЕДЫВАТЕЛЬНЫХ ДАННЫХ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

В связи с несекретным характером информации из открытых источников, персонал, занимающийся сбором общедоступных данных, может начинать сбор справочной информации о зонах ответственности до получения официального военного приказа на развертывание. Разведывательное подготовка боевых действий (IPB) – это интеграционный механизм (процесс) для Сухопутных войск, который определяет информационные требования к разведке в открытых источниках.

СБОР ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ

3-1. Процесс сбора и анализа общедоступной информации используется для экономии сил и времени, что позволяет получить надежную и детальную информацию об изменяющейся обстановке (миссия, угроза, рельеф местности и погодные условия, войска и силы поддержки, временные сроки, человеческий фактор – METT-TC) и оперативных факторах (политических, военных, экономических, социальных, информационных, инфраструктуры, физической среды, времени – PMESII-CT). При подведении итогов процесса принятия военных решений и разведывательной подготовке боевых действий (IPB) необходимо учитывать распоряжения командира для составления списка недостающих разведданных и информации. Видение командира:

- выражается в форме: описывать, (визуально) представлять и направлять;
- является основным руководством для разведывательного подразделения;
- проверяет полученные данные и информацию на соответствие

разведывательным требованием.

3-2. Видение командира выражается в форме информационных требований командира (CCIRs) и классифицируется в виде информационных требований дружественных сил (FFIRs) и приоритетных требований разведки (PIRs). Для сбора необходимой общедоступной информации, разведывательному подразделению требуется использовать продолжительные методы анализа и обработки информации, совместно с информационно-разведывательными требованиями и видением командира. Процесс сбора разведанных включает в себя сбор, обработку и представление информации в соответствии с поставленными задачами.

Собранная информация является основой разработки разведывательных баз данных, предоставления разведанных и ситуационной осведомленности.

3-3. Ведение разведки в открытых источниках является частью процесса планирования разведывательной подготовки к боевым действиям.

Персонал, принимающий участие в ведение разведки в открытых источниках, должен инициировать сбор и отправку запросов на получение детальной информации для соответствия информационным требованиям руководства. Сбор общедоступной информации включает в себя четыре шага (см. рисунок 3-1):

- Определение требований к информационным и разведывательным данным;
- Классификация требований к разведке;
- Определение источников для сбора информации;
- Определение методов сбора информации.

Определение требований к информационным и разведывательным данным

3-4. Нехватка информационных и разведывательных данных выявляется в ходе процесса разведывательного обеспечения тактических действий. Данные пробелы устраняются в соответствии с поставленной задачей и изменяющимися оперативными факторами в целях обеспечения руководства необходимой информацией. При поступлении разведанных, сотрудники OSINT вносят обновления в порядок разведывательного обеспечения

тактических действий и информируют командира обо всех изменениях оперативной обстановки.

Примечание. Ведение разведки в открытых источниках не может устранить все неизвестные аспекты и факторы, которые необходимы для командования. Заместитель начальника штаба или офицеры штаба должны быть готовы к заполнению данных пробелов с помощью методов анализа и прогнозирования. После дополнения информации, офицеры штаба должны приступить к разработке баз данных на уровне подразделения для предоставления общего доступа к ним. Это уменьшает количество новых запросов на предоставление необходимой информации от подчиненных подразделений и частей.

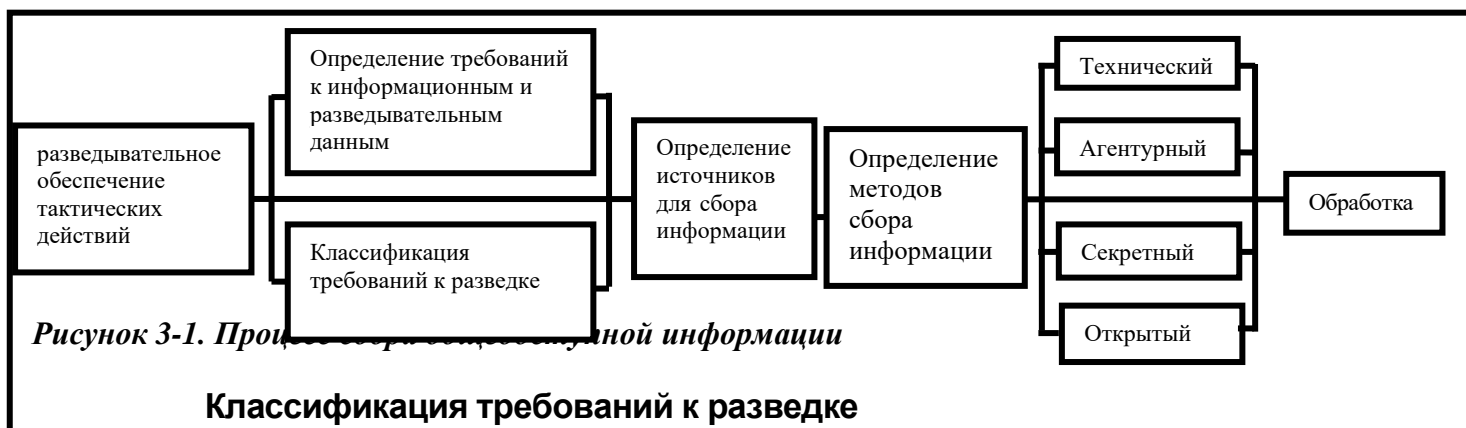


Рисунок 3-1. Процесс классификации требований к разведке

3-5. Требования разведывательного органа могут выходить за пределы сферы деятельности OSINT, что приводит к нехватке разведданных. Для устранения данных пробелов в разведке OSINT необходимо использовать подходящие методы.

3-6. Процесс разведывательного обеспечения тактических действий используется для классификации информационно-разведывательных требований по видам, основанным на анализе миссии и плане действий дружественных сил. Сотрудники OSINT предоставляют основную информацию на данном этапе. При ведении OSINT часто используются два важных термина – *частная (личная)* и *общедоступная* информация:

- **Частная (личная) информация** включает в себя общие сведения, факты, инструкции и другие материалы, относящиеся к конкретному лицу, группе или организации.

Требования разведывательного органа, требующие использования подобной информации не относятся к ведению OSINT. Кроме того, данная

информационная категория имеет две подкатегории:

- *Контролируемая несекретная информация* по различным причинам требует применения элементов управления и применения защитных мер (чувствительная, но несекретная информация или только для служебного пользования).

- *Секретная информация* нуждается в защите от несанкционированного использования. В связи с этим при разработке и распространении подобных документов необходимо указывать их гриф секретности.

- **Общедоступная информация** включает в себя сведения, факты, инструкции и другие публикуемые или транслируемые материалы для всеобщего обозрения. Подобная информация доступна по запросу общественности; находится на законном обозрении и слушании случайного наблюдателя; доступна на открытой для широкой общественности встрече.

Примечание. Количество секретной информации может быть ограничено и выделено из контекста, если данная информация рассматривается в виде секретных данных. При работе с большим количеством секретной информации необходимо подтверждение достоверности данной информации в открытых источниках. Подтверждение достоверности информации с помощью разведки в открытых источниках применяется для подтверждения надежности секретных источников, а также когда секретные источники недоступны.

Данный процесс подтверждает необходимость осуществления OSINT для оказания постоянной поддержки всех видов разведки.

Определение источников информации

3-7. Определение источника является частью требований к планированию и оценке процесса сбора общедоступной информации. Существует два типа источников, используемых для сбора информации – это *конфиденциальные* и *открытые* источники:

- **Конфиденциальные источники** могут являться отдельными лицами, группами или системой, которые обеспечивают защиту информации и соответствующих данных от публичного рассекречивания. Информационно-разведывательные требования, которые требуют использования конфиденциальных источников, не относятся к разведке OSINT.

- **Открытые источники** состоят из отдельных лиц или групп людей, которые предоставляют информацию, не требующей соблюдения авторских прав и

конфиденциальности. Подобная информация и относящиеся к ней данные не защищены от использования в открытых источниках. Виды источников:

- Академические источники. Программное обеспечение автоматизированного обучения, диссертаций, лекций, презентаций, научные статьи и исследования в печатном и электронном виде на темы экономики, географии (физической, культурной и военно-политической), международных отношений, региональной безопасности, науки и технологии.

- Государственные учреждения и неправительственные организаций. Базы данных, размещенная в открытых источниках информация, и печатные доклады по широкому кругу вопросов (экономика, экология, география, гуманитарная помощь, безопасность, наука и технология).

- Коммерческие и государственные информационные службы. Телевещание, публикация, и печатные новости на актуальные международные, региональные и местные тематики.

- Библиотеки и научно-исследовательские центры. Печатные документы и цифровые базы данных на различные тематики.

- Индивидуальные личности и группы. Рукописная, печатная, изобразительная, и транслируемая информация, основанная на искусстве, граффити, листовках, плакатах, татуировках и веб-сайтах.

- Серая литература (данные не доступные по обычным каналам). Информация, которая собирается с использованием передовых методов поиска в Интернете в сети Deep Web, а также состоящая из технических данных, научных трудов и официальных документов.

Определение методов сбора информации

3-8. Под термином «предварительный сбор» информации подразумевается получение необработанных сведений, на основе которых подготавливаются разведывательные данные. Собранная информация анализируется и совмещается с ранее полученными разведывательными данными. Эти данные включены в стандартную оперативную инструкцию, оперативный приказ и иные разведывательные механизмы обратной связи. Подобные методы гарантируют наличие определенных целей, а также обеспечивают базовой информацией об источниках и их деятельности в оперативной обстановке для прогнозирования развития ситуации и проверки оперативных данных. При сборе разведывательных сведений необходимо указывать цели противника, приоритет важности, временные сроки

вероятного события, временные рамки, в которых данная информация имеет значение (LTIOV), а также использовать методы запроса необходимой информации и подготавливать инструкции для личного состава.

3-9. Информация из открытых источников, соответствующая требованиям командира по предоставлению необходимой информации (CCIR) моментально должна распространяться среди командующего и другого персонала штаба через стандартную оперативную инструкцию или оперативные приказы. Методы сбора информации, в зависимости от сложности проводимой операции, могут повышать шансы соответствия информационно-разведывательным требованиям. При ведении OSINT можно использовать разнообразные методы, в том числе и технические средства.

3-10. Персонал по ведению OSINT обязан предоставлять материал в соответствии с требованиями разведки и установкой по получению информации из открытых источников. Сбор информации из открытых источников подразумевает получение данных в общедоступном (публичном) домене.

Степень, в которой открытые источники позволяют добывать ценную информацию, зависит от характеристик цели и необходимых данных.

Следует отметить, что необходимую информацию можно собирать из книг и журналов, вести наблюдение во время военных парадов, а также с помощью записи телевизионных и радиопрограмм.

ИССЛЕДОВАНИЕ ДАННЫХ

3-11. После определения методов сбора информации, персонал OSINT проводит исследование полученных сведений на соответствие информационно-разведывательным требованиям.

3-12. Подобные исследования:

- ведут к накоплению информационных и разведывательных баз данных. Эти базы данных позволяют персоналу OSINT своевременно реагировать на изменения в обстановке путем предоставления соответствующей разведывательным требованиям информации;

- используются для сбора информации, которая обеспечивает полное понимание проблемы и помогает в составлении картины общей оперативной обстановки;

- используются для накопления данных до и в ходе развертывания войск.

3-13. Существуют два типа (метода) исследования данных:

• *Оперативные исследования.* Сотрудники академических, правительственных, межправительственных и неправительственных организаций получают данные от первоисточника, также как и от вторичных источников. В свою очередь, данный метод достигается:

- Наблюдением одного из участников мероприятия, сбором данных и проведением опросов;

- Обычно проводится на оперативном и стратегическом уровнях для обеспечения командиров ситуационной осведомленностью, когда время не является основным фактором, влияющим на развитие информационных и разведывательных оперативных изменений (PMESII-PT).

• *Практические исследования.* Сотрудники разведывательных подразделений получают существующие данные и информацию от вторичных источников. Практические исследования:

- Обычно проводятся на тактическом уровне для обеспечения командиров ситуационной осведомленностью, когда время является одним из факторов, влияющим на развитие информационных и разведывательных изменений операции (METT-TC);

- Используются в основном среди сотрудников спецслужб, которые участвуют в ведении разведки в открытых источниках.

3-14. Все исследования начинаются с определения основного вопроса (причины) и разработки плана исследования.

Определение основной темы исследования

3-15. Исследование данных начинается с определения основной темы исследования, которая выражается в форме требований командира по предоставлению необходимой информации по данному вопросу.

При ведении разведки в открытых источниках, тема исследования может основываться на значимости цели и оперативной обстановки операции, а также совершенствоваться в соответствии с изменением информационно-разведывательных требований. Информационно-разведывательные требования, которые не получили соответствующих ответов подлежат

дальнейшему рассмотрению в процессе планирования и оценки плана сбора информации, в котором может быть использовано больше технических средств.

Разработка плана исследования

3-16. Различные аспекты в определении основной темы исследования могут быть выражены в форме информационно-разведывательных требований. Данные требования формируют основу для разработки плана исследования. План исследования может использовать оперативные и практические методы исследования данных. Данный план состоит из:

- определения источников информации (первичных и вторичных);
- описания процесса получения доступа к этим источникам;
- установления общего формата для базы данных;
- распространения данного формата всем подразделениям;
- определения методологии исследования.

Применение плана исследования

3-17. При использовании медиа-ресурсов, сотрудникам OSINT необходимо применять план исследования для использования средств передачи, приема и записи информации, а также различных компонентов и связанных с ними элементов (см. таблица 3-1). Первичные СМИ, используемые для реализации плана исследования включают:

- публичные выступления на форумах (конференциях и т.д.);
- общедоступные документы;
- общественное теле- и радиовещание;
- Интернет веб-сайты.

Примечание. В таблице не указан полный список открытых источников, однако указаны категорий общедоступных медиа-ресурсов, необходимых при сборе информации из открытых источников.

Таблица 3-1: Общедоступные медиа-ресурсы, компоненты и элементы

Источник	Компоненты	Элементы
-----------------	-------------------	-----------------

общедоступной информации		
Публичные выступления на форумах (конференциях и т.д.)	Выступающий	<ul style="list-style-type: none"> • Спонсор; • Взаимосвязь; • Главная мысль послания.
	Формат	<ul style="list-style-type: none"> • Конференция; • Дебаты; • Демонстрация; • Выступление; • Лекция; • Митинг (ралли); • Толк-шоу.
	Аудитория	<ul style="list-style-type: none"> • Место; • Состав.
Общедоступные документы	Графика	<ul style="list-style-type: none"> • Рисунок; • Гравюра; • Картина; • Граффити; • Фотография; • Печать; • Постер.
	Запись	<ul style="list-style-type: none"> • Устройство для хранения компактных данных; • Цифровой видеодиск; • Жесткий диск; • Кассета.
	Печать	<ul style="list-style-type: none"> • Книга; • Брошюра; • Газета; • Журнал; • Публикация государственных документов;

		<ul style="list-style-type: none"> • исследование содержимого мусорных контейнеров «Dumpster diving» • Ежегодные послания; • Периодические издания; • Каталог; • Доклад; • Новинки; • Публикация негосударственных документов; • Листовка; • Бизнес карта.
Общественное теле- и радиовещание	Радио	<ul style="list-style-type: none"> • Низкочастотное АМ-Радиовещание; • Среднечастотное АМ-Радиовещание; • Радиовещание на коротких Волнах; • FM-Радиовещание в ОВЧ (VHF) диапазоне; • Спутниковое радиовещание; • Радиовещание на стандартных волнах.
	Телевидение	<ul style="list-style-type: none"> • Спутниковое телевидение в Ku-диапазоне; • Эфирное телевидение в ОВЧ (VHF) и УВЧ (UHF) диапазонах; • Реклама; • Кинематография.
Интернет-ресурсы	Связь	<ul style="list-style-type: none"> • Чат; • E-mail (электронная почта); • Новости; новостные группы; • Веб-камера; • Веб-вещание; • Веб-блог (журнал, дневник, форум).
	Базы данных	<ul style="list-style-type: none"> • Коммерция;

		<ul style="list-style-type: none"> • Образование; • Государство; • Военные организаций.
	Информация (содержание веб-страницы)	<ul style="list-style-type: none"> • Коммерция; • Образование; • Государство; • Военные организаций.
	Услуги	<ul style="list-style-type: none"> • Словарь; • Справочник; • Загрузки; • Финансы; • Геопространство; • Общий поиск и поиск URL-адреса (ссылки); • Техническое обеспечение; • Перевод.
AM – амплитудное модулирование FM – частотное модулирование UHF – ультравысокие частоты		URL – унифицированный указатель ресурса (источника) VHF – очень высокие частоты

Публичные выступления на форумах

3-18. Сотрудники OSINT занимаются разведывательной деятельностью при посещении публичных форумов, в частности: конференций, лекций, общественные митинги и демонстраций, рабочие группы и дебаты.

Посещение подобных мероприятий позволяет строить отношения с невоенными специалистами и организациями. От сотрудников разведывательного органа требуется глубокое познание местной культуры и законов с целью обеспечения легитимности (законности) действий по сбору информации для соблюдения местных обычаев или законов (пример: правило «Chatham House Rule» – конфиденциальность источника информации). При проведении операции по сбору общедоступной информации, рекомендуется

согласовывать свои действия с начальником военно-юридической службы для соблюдения правил «AR 381-10, процедура 10» (U.S. Army Intelligence Activities – Деятельность военной разведки США от 3 мая 2007 г.). Следует отметить, что ситуационная осведомленность и понимание местной культуры достигается с помощью создания военных и невоенных контактов с посетителями, а также определения интересующих лиц на данных мероприятиях и выявления любых изменений в выступлении спикера.

3-19. Обычно сотрудники OSINT посещают публичные выступления и форумы, связанные с операциями по стабилизации обстановки или операциями против повстанцев, на которых уровень опасности минимален.

Примечание. Правило «Chatham House Rule» гласит: «Если встреча, или ее часть, проходит в рамках данного правила, то участники мероприятия могут свободно использовать полученную информацию, однако они не могут использовать информацию личного характера (идентификационная), принадлежность (связь) выступающего (спикера) и других участников. Соблюдение правила «Chatham House Rule» должно быть согласовано до начала проведения мероприятия. Применение «Chatham House Rule» изменяет характеристику источника от открытого (общедоступного) до конфиденциального, а также может потребовать ограничений в сборе информации для соблюдения ограничений разведывательной деятельности (См. приложение А).

Общедоступные документы

3-20. При приобретении официальных общедоступных документов, сотрудники OSINT должны быть осведомлены об обстановке и использовать законные методы, подходящие для данной ситуации. Эти методы включают, но не ограничиваются:

- фотографированием и копированием документов, предоставленных на общественных форумах, в частности, городских холлах, библиотеках и музеях;
- поиском среди выброшенных документов в общественных местах (улицы, рынки и туалеты);
- фотографированием документов в общественных местах (баннеры, граффити и плакаты);
- покупкой документов у уличных торговцев, а также в газетных киосках, книжных магазинах и издательствах;

- покупкой документов через третьи лица (оптовый дистрибьютор или участник книжного клуба);
- получением документов по запросу от авторов, конференций, ярмарок, прямой почтовой реклама.

Общественное теле- и радиовещание

3-21. Региональные бюро Директора национальной разведки Центра открытых источников занимается сбором информации на региональных и международных сетях вещания, в соответствии с требованиями разведки в открытых источниках. Охват регионального и международного вещания позволяет сотрудникам OSINT и разведывательным организациям использовать знакомые источники. Для получения информации из общественного вещания используются четыре метода:

- *Спектральный поиск.* Поиск по всему спектру частот для обнаружения, определения (идентификации) и выявления местонахождения всех излучателей сигнала, которые могут подтвердить общие сведения. Подобный поиск дает обзор количества и видов источников, а также их расположения в спектре;

- *Поиск диапазона частот.* Поиск определенного сегмента в спектре частот для подтверждения общих сведений об источнике. С помощью определения отрезка частот можно повысить вероятность получения сигнала;

- *Поиск частот.* Поиск радио- или телевизионных частот;

- *Поиск программ.* Поиск радио- или телевизионных программ. При этом программы различаются по типу, характеристике содержания и медиа формату. Разведка через программное вещание устанавливается и расширяется при получении первоначальных результатов.

Примечание. Для достижения эффективных результатов, сотрудники OSINT должны использовать данные методы в комплексе (совместно). Выбор методов зависит от миссии, численности и возможностей подразделения.

3-22. Более подробную информацию по сбору данных из общественного вещания можно получить в Центре открытых источников Директора национальной разведки.

Интернет-ресурсы

3-23. Существуют четыре последовательных шага для получения

информации из Интернет-ресурсов:

- Составление плана поиска;
- Проведение поиска;
- Совершенствование техники поиска;
- Сохранение (запись) результатов поиска.

3-24. Более подробную информацию об исследованиях с использованием Интернет-ресурсов можно найти в приложении С.

ГЛАВА 4

ПРОВЕДЕНИЕ РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ

Сухопутные войска оперируют по всему миру в различных условиях. Такое разнообразие требует правильного и эффективного использования общедоступной информации из открытых источников. Учитывая объем существующей общедоступной информации и непредсказуемости запросов информационно-разведывательных требований, сотрудники OSINT для проведения разведки в открытых источниках должны быть высококвалифицированными и гибкими. Эффективное проведение разведки в открытых источниках гарантирует, что командиры и подчиненные получат своевременные, актуальные и точные разведданные. Сотрудники OSINT проводят разведку путем оценки, анализа, подготовки отчетов и распространения разведданных в форме оценок, исследований и прогнозов.

КАТЕГОРИЙ РАЗВЕДЫВАТЕЛЬНЫХ ДАННЫХ

4-1. Разведывательные и информационные требования определяются в результате анализа полученной миссии через процесс принятия решений и распоряжений командира (описывает, визуализирует и формирует приказы). Сотрудники, ведущие разведку в открытых источниках, осуществляют сбор информации, проводят анализ, подготавливают материал и распространяют его в соответствии с категориями разведданных (см. таблицу 4-1). Подготовленные материалы классифицируются по назначению и цели. Некоторые категорий могут

совпадать. Одна общедоступная информация может быть использована при составлении нескольких разведданных.

Таблица 4-1. Категорий разведывательных данных

<i>Индикаторы и предупреждения</i>
<i>Индикаторы и предупреждения</i> являются разведывательной деятельностью, направленной на определение и сообщение о срочной разведывательной информации и действиях зарубежных стран, которые могут включать в себя угрозу для США, его союзников или граждан за рубежом. Она включает в себя предупреждение о враждебных действиях или намерениях, направленных против США, его деятельности, зарубежных или коалиционных сил НАТО.
<i>Текущие разведывательные данные</i>
<i>Текущие разведывательные данные</i> оказывает непосредственную поддержку проходящим в настоящее время операциям. Она включает в себя процесс интеграции срочной информации, а также данных, поступающих из всех видов разведки, в целях составления кратких, точных и объективных разведывательных справок о регионе проведения операции и существующих в ней угрозах. Офицер разведки отвечает составление текущих разведывательных данных для подразделений. В дополнение к текущей ситуации, текущие разведывательные данные должны содержать прогнозы о возможных угрозах и их последствиях.
<i>Общая военно-разведывательная информация</i>
<i>Общая военно-разведывательная информация</i> включает в себя сведения: о военном потенциале зарубежных стран, возможности вооруженных сил и их характеристике, структуре, системе подготовки, тактике, военной доктрине, стратегии и другие факторы, влияющие на проведение военной операции, ее эффективность, разведывательную деятельность на местности (за исключением научно-технической разведки). Эта категория, как правило, связана с долгосрочным планированием на национальном уровне.
<i>Разведывательные данные о цели</i>
Разведка, которая определяет все важные компоненты объекта и указывает на его уязвимые и относительно важные элементы. Составление разведывательных данных об объекте является анализом подразделений

противника, его расположения, его возможностей и системы с целью выявления и выбора конкретных целей или уязвимых мест для осуществления атаки, контратаки или захвата.

Данный процесс состоит из изучения цели и анализа боевых возможностей. Изучение цели является систематической оценкой и анализом целевых систем, его компонентов, а также составных элементов для определения важных объектов для потенциального взаимодействия посредством смертельных и нелетальных средств. Анализ боевых возможностей дает своевременные и точные оценки последствий применения военной силы и войны.

Научно-техническая разведка

Научно-техническая разведка является результатом сбора, оценки, анализа и интерпретации иностранной научно-технической информации. Научно-техническая разведка охватывает зарубежные разработки в области фундаментальных и прикладных научных исследований и прикладных инженерных методов и научно-технических характеристик, возможностей иностранного военного оружия, систем вооружения и техники, научных исследований и разработок, а также методов производства, используемых для их изготовления.

Контрразведка

Процесс сбора информации и осуществление деятельности, направленных на выявление, дезинформирование, использование, разрушение и защиту от шпионажа, разведывательных действий, саботажа или убийства, проводимых в интересах или от имени иностранных государств, организаций, лиц, агентов или международных террористических организаций. Контрразведка анализирует угрозы, исходящие от иностранных разведок и служб безопасности, а также международных террористических организаций и разведывательных действий негосударственных структур, таких как организованная преступность, террористические группы и наркоторговцы.

Разведывательная информация на основе оценочного анализа

Разведка, которая определяет, описывает и дает прогнозы о возможностях противника и последствиях планирования и проведения военных операций. Разведывательная информация на основе оценочного анализа выходит за рамки описания возможностей угрозы или его

деятельности, а пытается предсказать неизвестные угрозы на основе анализа известных фактов с использованием таких методов, как системный анализ, составление выводов и статистической вероятности.

АНАЛИЗ ИНФОРМАЦИИ

4-2. Открытые источники являются доступными и незасекреченными. В связи с этим, такие аспекты публично доступной информации и открытых источников, как обман, предвзятость и дезинформация представляют особый интерес при оценке источников информации во время ведения разведки в открытых источниках. Информация оценивается с точки зрения:

- процесс общения;
- надежности и достоверности.

Процесс общения

4-3. Простой моделью процесса общения, как правило, является двустороннее общение, которое состоит из шести частей:

- преднамеренное сообщение;
- говорящий (отправитель);
- скрытый смысл сообщения говорящего;
- слушатель (ресивер);
- скрытый смысл сообщения слушателя;
- восприятие сообщения.

4-4. Как показано в таблице 4-2, спикер и слушатель имеют разные перспективы и аспекты коммуникации.

В ходе общения существуют проблемы, связанные с тем, что тратится большое количество времени на расшифровку слушателем закодированного сообщения (мысли).

4-5. Часто трудно оценить процесс общения во время публичных выступлений, потому что существуют множество элементов, которые могут помешать успешной передаче сообщения. В результате одновременного сочетания нескольких элементов, общественные выступления могут быть неправильно поняты.

4-6. Спикер передает целенаправленное сообщение, вкладывая свой смысл, устным или невербальными методами, голосовыми и визуальными средствами передачи информации или с помощью их комбинации.

Заложенный смысл может быть утрачен в ходе отправки сообщения, его распространения и получения. Полное понимание данного процесса обычно

позволяет эффективно обмениваться информацией между говорящим и слушателем.

4-7. Вербальное общение начинается с взаимного обмена мыслями, мнениями и информацией. Данное общение может быть *положительным* или *отрицательным*. Учитывая способы передачи сообщения, можно определить следующие психологические характеристики человека:

- пассивный;
- агрессивный;
- пассивно-агрессивный;
- настойчивый.

4-8. Люди передают информацию вербально и невербально на основе своих убеждений, эмоций и целей. Эти виды передачи информации, указаны в таблице 4-2. Для эффективной передачи информации (общения) и во избежание недоразумений, важно понимать различия в стиле общения и как они воспринимаются аудиторией. Применение таблицы для сравнения методов передачи информации может помочь сотрудникам, занимающимся ее сбором, определить влияние окружающих факторов (других людей) на содержание данной информации и предсказать ее восприятие общественностью. Таблица 4-2 иллюстрирует и предоставляет основные положения, которые помогут определить поведение, убеждения, эмоций и цели человека.

Примечание. Таблица 4-2 предназначена для оказания помощи при ведении разведки во всех доступных источниках. Общедоступная информация и открытые источники используются для определения личности и его характерных черт (составление психологического портрета).

Психологические портреты составляются на основе предыдущих выступлений, лекций, проповедей или заявлений человека, с целью определения его дальнейших шагов, решений и реакций. Существуют внешние условия, которые могут положительно или отрицательно влиять на человека: последствия конфронтации с мнениями вышестоящего руководства, окружающая обстановка (научная, религиозная или политическая), или импровизированное общественное интервью в формате вопросов и ответов.

НАДЕЖНОСТЬ И ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ

4-9. Сотрудники OSINT постоянно оценивают надежность и достоверность информации. Определение надежности открытых источников является важным и необходимым условием для определения цели информации, дезинформации и

обмана. Рейтинг надежности составляется на основе субъективных суждений аналитика, и точности (достоверности) предыдущей информации из этого же источника.

4-10. Сотрудники OSINT должны оценить надежность и достоверность информации, независимо друг от друга, чтобы избежать предвзятости. Существует три типа источника, используемые для оценки и анализа полученной информации:

- первичные источники. Имеют прямой доступ к информации, и передают ее полностью без искажений.

- вторичные источники. Передает информацию со ссылкой на другие источники, используя прямую речь или кратко пересказывая информацию.

- авторитетные источники. Точно сообщают информацию, поступающую от главы государства, правительства или правящей партии.

Примечание. Вторичные и авторитетные источники, в частности правительственные пресс-службы, коммерческие новостные организации, политические штабы, публикаций научно-исследовательских центров, газеты, периодические издания, базы данных и библиотеки, могут умышленно или неумышленно добавлять, удалять, изменять или фильтровать информацию, представленную общественности.

	Пассивный	Агрессивный	Пассивно-агрессивный	Настойчивый
Поведение	<ul style="list-style-type: none"> • Молчит. • Не говорит, что на самом деле чувствует, необходимо или хочет. • Часто имеет низкую самооценку. • Приносит извинения, если 	<ul style="list-style-type: none"> • Выражает чувства и желания, как будто другие способы необоснованы или глупы. • Отклоняет, игнорирует или оскорбляет потребности, желания и 	<ul style="list-style-type: none"> • Не соответствует ожиданиям других людей в результате «отказа» (забывает или откладывает выполнение чего-либо). • Отрицает ответственность за свои 	<ul style="list-style-type: none"> • Выражает потребности, желания и чувства прямо и честно. • Позволяет другим иметь свои взгляды без увольнения или оскорбления.

	<p>выражает свое мнение.</p> <ul style="list-style-type: none"> •Отрицает чувства разногласия или равнодушие. 	<p>мнения других людей.</p>	<p>действия.</p>	
Невербальное общение	<ul style="list-style-type: none"> • Минимизирует себя. • Смотрит вниз, разводит руками, избегает зрительного контакта. • Говорит тихо. 	<ul style="list-style-type: none"> •Увеличивает себя и кажется угрожающим. •Зрительный контакт является фиксированным и проникающим. • Голос громкий, возможно, крикливый. 	<ul style="list-style-type: none"> •Как правило, имеет пассивную мимику. 	<ul style="list-style-type: none"> •Тело расслаблено, движения являются случайными. •Зрительный контакт является частым, но не ярким.
Убеждения	<ul style="list-style-type: none"> •Другие потребности являются более важными. • Другие имеют больше прав. • Вклад других является более ценными. 	<ul style="list-style-type: none"> •Личные потребности являются более важными и более оправданным, чем других. •Другие не имеют личных прав. •Личные взносы 	<ul style="list-style-type: none"> •Выбирает собственный путь, даже после принятия обязательств перед другими. •Не несет ответственности за личные действия. 	<ul style="list-style-type: none"> •Потребности каждого человека одинаково важны. •Каждый человек имеет равные права быть выразительным. •Каждый человек имеет ценный вклад.

		являются более ценными.		•Отвечает за личное поведение.
Эмоции	<ul style="list-style-type: none"> • Отказываетс я от страха. • Чувствует себя беспомощны м, разочаровани е и гнев. •Медведи обижаются на жестокое обращение других. • Имеет низкое самоуважени е. 	<ul style="list-style-type: none"> • Сердитый или сильный в момент победы. •Чувствует угрызение совести, чувство вины или ненависть к себе за причинение вреда к другим. 	<ul style="list-style-type: none"> •Бойтс я уверенности в себе. •Возмущаетс я требованиями других. • Опасаетс я, что ему противостоят 	<ul style="list-style-type: none"> • Положительные чувства о себе и других. • Высокий уровень самооценки.
Цели	<ul style="list-style-type: none"> •Избегает конфликтов. •Радует других любой ценой. •Дает другим руководить. 	<ul style="list-style-type: none"> •Побеждает любой ценой для других. •Получает контроль над другими. 	<ul style="list-style-type: none"> •Получает личный путь без принятия на себя ответственности. 	<ul style="list-style-type: none"> •Самоуважение хранится всеми. •Выражает себя без нужд все время побеждать. •Никто не контролирует никого.

4-11. Неавторитетным источникам не хватает надежности и достоверности, и они редко выделяются из авторитетных источников.

4-12. Неавторитетные источники, как правило, недоступны для
Исследовательский Центр Виктора Воксанаева
Бюллетень OSINT № 33 (сентябрь – октябрь 2013 г.)

общественности. Не имеют подтверждения несколькими публичными источниками информации. Примеры неавторитетных источников:

- Документы из веб-хранилищ, такие как блоги, Wikipedia, политические сайты и коммерческие рекламы.

- Материалы, полученные через неподтвержденные электронные почты, понаслышке, или заявления исключительно в устной форме.

- Неофициальные личные связи, такие как письма в редакцию, эссе и мнения.

4-13. При оценке источников информации для определения ее достоверности необходимо рассмотреть:

- **Идентичность.** Источник информации (студент, учитель, политическая организация или репортер)?

- **Полномочия.** Как хорошо источник знаком с информацией?

- **Мотив.** Почему публикуется данная информация?

- **Доступ.** Является ли источник непосредственным свидетелем события или информации?

- **Своевременность.** Дата информации?

- **Внутренняя и внешняя согласованность.** Противоречит ли информация государственной политике и понятиям местных жителей?

ПРОЦЕСС ОБРАБОТКИ ИНФОРМАЦИИ

4-14. Процесс представляет собой деятельность по управлению информацией, направленной на повышение степени значения информации от просто данных до разведывательных справок. Функция обработки, хотя и не является составной частью разведывательного процесса, но является важным элементом при анализе и проведении разведки в открытых источниках. Общедоступная информация соответствует информационно-разведывательным требованиям. В зависимости от типа полученной информации до опубликования и распространения она должна быть обработана. Сотрудники спецслужб преобразовывают общедоступную информацию и открытые источники в форму - пригодную для обработки:

- оцифровка (выражение в цифровой форме);

- расшифровка и перевод.

Оцифровка

4-15. Сотрудники OSINT создают цифровые записи документов путем сканирования или создания фотографии. Соответствующая информация о

документе должна быть создана для обеспечения подотчетности и облегчения ее поиска. Оцифровка позволяет распространять документы во внешние базы данных и организаций, а также позволяет использовать инструменты машинного перевода для поиска документов по ключевым словам, именам и фразам.

Запись и перевод

4-16. *Запись* является дословно записанным на оригинальном языке аудио- и видеоматериалом произнесенных слов. Для сохранения смысла информации, аудио материалы и записи на языке оригинала имеют важное значение. Запись включает в себя описание деятельности, историю и условия, которые переписчик слышит в аудио- и видит в видеоматериале. Лингвист использует онлайн-словари, справочники, аппаратуру, а также программное обеспечение для улучшения записи. После завершения записи, она проходит проверку качества.

4-17. *Перевод* является недословным, но приближенным прямым значением иностранного языка. Лингвист должен уметь читать и понимать исходный язык, писать понятно на английском языке, а также уметь выбрать эквивалентные выражения на английском языке, которые полностью передают и соответствуют смыслу исходного материала.

4-18. Во время обработки, лингвист подготавливает аннотацию или осуществляет полный перевод оригинального документа. Лингвист использует онлайн-словари, справочники, аппараты и программное обеспечение для улучшения качества перевода. После завершения, перевод отправляется на проверку качества.

4-19. Лингвисты осуществляют проверку качества каждой записи и переводов в целях подтверждения качества и согласованности с установленными процедурами действия подразделений. Представители правительства США или военные переводчики должны перепроверять все материалы, подготовленные неамериканскими переводчиками, за исключением, если данный перевод был составлен представителями союзнических стран или американскими подрядчиками, имеющих богатый опыт и высокую квалификацию.

Лингвистическая проверка качества является важным аспектом в процессе обработки иностранной общедоступной информации. Каждая запись и перевод проходит два уровня проверки:

- **проверку качества.** Во время проверки качества, квалифицированный лингвист убеждается в том, что запись или перевод содержит точную, полную и не имеющую искажений информацию, которая соответствует всем стандартам.

Лингвист возвращает запись или перевод для коррекции, добавляет и исправляет пропущенное содержание, исправляет мелкие ошибки. После завершения проверки качества запись или перевод можно использовать для обработки.

- **гарантирование качества.** Для гарантирования качества, квалифицированный лингвист или аналитик OSINT проверяет запись или перевод на наличие всей необходимой информации в содержании документа. После завершения проверки окончательный вариант записи или перевода сохраняется во внутренней базе данных, которую в дальнейшем можно обработать, использовать при составлении разведывательных документов и распространять.

Анализ источника информации

4-20. Процесс анализа средств массовой информации состоит из систематического сопоставления содержания, поведения, формата и тенденций основных средств массовой информации и информационных источников страны. Анализ средств массовой информации- как вид деятельности был сформирован на основе методов и опыте, накопленного в ходе проведения разведки в открытых источниках против авторитарных политических систем во время Второй мировой войны и Холодной войны, когда средства массовой информации находились под прямым контролем правительства. Для эффективного осуществления разведки в открытых источниках общедоступная информация и открытые источники должны быть проанализированы. При оценке аналитического материала сотрудники OSINT используют три критерии оценки информации. Эти критерий помогают сотрудникам OSINT различать факты, показатели, модели и тенденций в области информации и взаимоотношений. Это включает в себя индуктивное или дедуктивное рассуждение необходимое для полного понимания смысла прошедших и предсказания будущих событий.

4-21. Сравнение тенденций в содержаниях отдельных средств массовой информации с изменениями официальной политики страны позволяет определить прогосударственные СМИ. Составляя справку о прошлой деятельности средств массовой информации, которые при следовании центральной политики страны уязвимы перед внешним и внутренним факторами, сотрудники могут выявить потенциальные изменения в политике государства. Сравнение уже сказанного и еще не сказанного на фоне того, что говорят другие и того, что было сказано вначале, является основой анализа информационного

источника.

4-22. Процесс анализа среды СМИ, в которой присутствуют как официальные так и неофициальные СМИ, является важным процессом.

Официальные средства массовой информации могут находиться под давлением государства и следовать за центральной политикой страны. При проверке средств массовой информации анализу должны подвергаться как журналисты так и комментаторы. Очень важно создать справку (досье) о журналистах и комментаторах, что откроет доступ к «инсайдерской» информации государственных структур или сведений, используемых должностными лицами для определения курса развития страны.

Примечание. Присутствие разной информации в контролируемых различными элитами СМИ, помогает выявить политические и внутриэлитные споры той или иной страны. Например, если сравнить комментарий к выступлению президента, опубликованные в контролируемых правительством СМИ и независимых медиа-ресурсов, то можно выявить много различий.

4-23. Существует три аспекта при анализе СМИ:

- Принадлежность;
- Структура;
- Содержание.

Принадлежность

4-24. Анализ сферы СМИ, с точки зрения его принадлежности, требует осведомленности сотрудников спецслужб о том, как действуют, влияют и представляют интерес различные информационные элементы. Тщательное изучение различий того, как используются средства массовой информации в различных условиях, может дать представление о внутренней и внешней стратегии правительства. Существуют следующие классификации СМИ:

- находятся под контролем правительства;
- централизованное управление над средствами массовой информации;
- доминирующим элементом управления является правительство и политические руководители высокого уровня;
- правительство для осуществления контроля над содержанием СМИ до распространения информации используют механизм цензуры;
- находится не под полным контролем;
- контроль над СМИ является полу-централизованным;

- до распространения информации правительство, оказывая давление на руководителей СМИ и журналистов, использует механизм самоцензуры;

- независимые;

- децентрализованный контроль над СМИ;

- правительства может регулировать частоту вещания, нравственное содержание, право владения, а иногда оказывает политическое давление на информагентства и журналистов;

- экономические факторы, нормы журналистской профессии, предпочтения людей, которые управляют информагентствами и качества отдельных журналистов, которые сообщают или комментируют ту или иную новость - все это оказывает влияние на содержание СМИ.

4-25. Все СМИ, в какой-то степени, находятся под чьим-либо контролем и в результате этого спецслужбам легче осуществить анализ медиа-источника. Основной задачей сотрудников OSINT является определение уровня, факторов и элементов, находящихся под контролем элит, учреждений или отдельных лиц (степень их влияния) и какие области представляют интерес для соответствия информационно-разведывательным требованиям спецслужб.

Уровень	Фактор	Элементы
Политический	Законы и нормы, регулирующие деятельность СМИ, должностных лиц и использование полномочий	Консенсус высшего руководства Индивидуально каждого лидера Учреждения
Журналист	Степень свободы СМИ, предоставленной политической системой	Совет директоров медиа-компаний Индивидуальные директоры Влиятельные акционеры Управление редакторов Департамент редакторов Производители программы Сильнейшие индивиды Журналисты

Личность	Законы и нормы, регулирующие внешний вид и поведение отдельных лиц в СМИ	Группа субъектов или участников Индивидуальный субъект или участник

Структура СМИ

4-26. Структура СМИ включает в себя атрибуты медиа-материалов. Существуют структурные элементы, которые влияют на смысл и значение содержания. Анализ этих элементов раскрывает понимание точек зрения сотрудников в контролируемых правительством, частично контролируемых и независимых СМИ и позволят определить структуру медиа-элементов.

4-27. Структурные элементы СМИ:

- процесс отбора, обработки и точка зрения;
- иерархия власти СМИ;
- определение формата;
- типы медиа-ресурсов;
- важность;
- распространение;
- временные параметры.

Процесс отбора, обработки и определения точки зрения

4-28. Процесс выбора информации для опубликования в новостях возложено на редакцию. Он включает в себя решение руководителя отдела информагентства о том, какие истории уже опубликовывались, а какие необходимо опубликовать. Руководитель определяет форму подачи информации (вкладывая необходимую точку зрения), какие изображения включить, значение какой мысли необходимо усилить или приуменьшить.

Иерархия власти СМИ

4-29. Все политические системы состоят из иерархии власти, которая логически следует за официальными заявлениями «элементов» (лидеров, политических руководителей и т.д.) в соответствии с иерархией авторитетности.

Авторитетность определяет то, что мнение, высказанное в заявлении, отражает доминирующую точку зрения в рамках политической системы. Структуру иерархии власти можно отчетливо увидеть на политическом уровне - заявление премьер-министра имеет больший политический вес, чем заявление министра. В других случаях, иерархия может быть не столь очевидным, выступление председателя партии является более авторитетным, чем главы государства.

Таблица 4-4. Иерархия власти СМИ

Тип информации	Цель	Пример
Отчеты	Информирует зрителя, слушателя или читателя	Отчет авторитетного или неавторитетного источника, основанный на характеризующих СМИ данных
Комментирование и редактирование	Сообщить о позиции и мнении государства, а также осуществить процесс убеждения зрителя, слушателя или читателя	<p>Комментаторы Заслуживающие внимания:</p> <ul style="list-style-type: none"> • Высшие руководители • Известные советники премьер-министра • Люди, имеющие связи с крупной политической партией • Эксперты <p>Редакторы Заслуживающие внимания:</p> <ul style="list-style-type: none"> • Лидеры правящей партии и крупные финансовые доноры • Большая часть политической или финансовой элиты • Большое число избирателей или

		небольшое количество участников выбора •Небольшой сегмент избирателей или населения с особыми интересами или радикальными взглядами •Местные должностные лица и граждане
Официальные заявления	Объявление курса внешней и внутренней политики страны должностным лицом или исполнительным органом правящей партии	Заслуживающие внимания: - Президент - Госсекретарь страны -Представитель государственного департамента

Определение формата

4-30. Определение формата является процессом выбора метода распространения информации для общественности через средства массовой информации. Информация может подаваться в виде репортажа или интервью в прямом эфире, предварительно записанных сообщений или интервью, что позволяет оказывать влияние на содержание информации, предоставляемой потребителям.

Типы медиа-ресурсов

4-31. По сравнению с другими видами СМИ телевидение имеет крупнейший потенциал и оказывает существенное влияние на формирование мнения среди населения. Телевидение заменило радио в качестве основного источника новостей, за исключением мест, где бедность не позволяет иметь доступ к нему. Некоторые люди могут получить информацию из газет и новостных интернет-сайтов, но эти люди могут быть богаче, образованнее и влиятельнее, чем общая телевизионная аудитория. Специализированные печатные издания и интернет-сайты все еще имеют маленькую аудиторию, но в эту аудиторию, скорее всего, будут входить должностные лица и специалисты, которые могут повлиять на политические дебаты и их результаты.

Важность

4-32. Вопросы помогающие определить важность появившегося в СМИ

сообщения:

- Где было опубликовано сообщение (на первой полосе газеты или домашней странице новостного интернет-сайта)?

- Предоставленный объем для опубликования сообщения?

- В каком порядке данное сообщение появляется в выпуске новостей?

- Показали ли его при предварительном показе основного выпуска новостей?

- Как часто данное сообщение ретранслировалось на последующих выпусках или периодических изданиях?

- Сколько времени эфирного времени он получил?

Распространение

4-33. В контролируемых правительством СМИ способ распространения заявлений руководителя страны имеет важное значение. Руководители стран общаются с населением с помощью различных форм передачи информации, таких как официальные политические заявления, официальные интервью, а также неожиданных высказываний. Сравнивая масштабы внимания СМИ к заявлению политического руководителя, можно определить его намерение о том как данное сообщение должно быть воспринято населением страны (в виде официального объявления политического курса или всего лишь временного, несогласованного сообщения).

Временные параметры

4-34. Сотрудники OSINT уделяют огромное внимание на время появления информации в СМИ, а также его вступление в цикл производства новостей. Цикл производства новостей является процессом и временным параметром, с помощью которых разные типы источников получения информации и СМИ, включают данную информацию в свои новостные материалы и создают из него доступную для общественности новость.

Медиа-контент

4-35. Понимание значимости содержания увеличивает полезность анализа источника информации. Медиа-контент включает в себя следующие элементы:

- Открытое содержание;

- Скрытое содержание.

Открытое содержание

4-36. Открытое содержание включает в себя слова, образы и звуки, передающиеся открытым источником. Одним из наиболее важных форм анализа медиа-ресурсов является тщательное сопоставление содержания авторитетных

официальных заявлений с целью определения скрытой в ней цели или намерения. В целях усиления, поддержания и укрепления политики страны правительства, политические организации и руководители часто публикуют свои заявления и информации в медиа-ресурсах.

4-37. Анализ открытого содержания авторитетных публичных заявлений является эффективным инструментом определения намерений и позиции руководства. Для эффективного понимания открытого (явного) содержания необходимо учитывать следующие методы общения:

- скрытое общение или «чтение между строк» являются частью публичных заявлений, поверхность которых не отражает реальную мысль, значение и цель автора. Использование методов скрытого общения часто встречается в политических системах, имеющих строгие запреты на распространение конфиденциальной информации среди населения или в случаях, когда щепетильные вопросы находятся под угрозой раскрытия.

- при анализе содержания опубликованной в СМИ информации, необходимо изучить не только содержание слов, но и мимику, интонацию и голос человека во время интервью или выступления, также требуется проанализировать оригинал информации и все имеющиеся в СМИ экспертные оценки. Эти данные помогут определить серьезность заявления политических руководителей.

- необходимо учитывать историю формирования и деятельности открытых источников. Такие средства воздействия, как СМИ, журналисты, ньюсмейкеры и новостные телекомпаний не могут находиться под постоянным контролем. Такие проблемы, как временные ограничения и технические неисправности активно влияют на содержание общественной информации. Решение аналитика о деятельности источника информации должно быть принято после тщательного изучения его предыдущей деятельности.

Скрытое содержание

4-38. Скрытое содержание - спрятанная идея или мысль в содержании информации. Глубокий анализ скрытого содержания может помочь определить основные особенности и действия людей, контролирующие средства массовой информации.

ПРОЦЕСС ПРЕДОСТАВЛЕНИЯ И РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

4-39. Информационные и разведывательные данные, прошедшие проверку через открытые источники, должны немедленно сообщаться и распространяться в установленном порядке действий (SOPs), который соответствует требованиям

разведки, а также степеням важности и секретности информации.

Примечание. Сотрудники разведывательного органа, непосредственно не занимающиеся ведением разведки в открытых источниках также получают информацию, которая необходима для каждого элемента данного органа. Тесное сотрудничество в подразделении способствует благоприятной среде для эффективного сбора, обработки и предоставления данных об оперативной и разведывательной обстановке по соответствующим каналам.

4-40. В случае если данные, прошедшие обработку, не своевременно и в неправильной форме предоставлены и распространены среди командующего и личного состава, то такая информация не несет никакой важности для разведки. Предоставление и распространение обработанных данных из открытых источников, соответствующих информационно-разведывательным требованиям включают, но не ограничены следующим:

- Однопрофильные или многопрофильные расчеты и оценки;
- Констатация фактов;
- Оценка возможностей и ограничений противника (угрозы);
- Вероятный оперативный план (COAs) противника.

Определение инструкций и методов

4-41. Эффективное распространение информации способствует созданию механизма обратной связи с целью выявления степени полезности и необходимых изменений в требованиях к разведывательной информации.

Основная цель в предоставлении и распространении разведданных заключается в обеспечении поддержки процесса проведения (планирования, подготовки, выполнения и оценки) операции.

4-42. Основные направления в подготовке разведданных, подлежащих предоставлению и распространению:

- **Своевременность.** Информация должна быть предоставлена соответствующим подразделениям без промедления.
- **Актуальность.** Информация должна отвечать на запросы разведывательных подразделений и частей. Соответствующая информация снижает расход времени на сбор, обработку и передачу информации.
- **Полнота.** Установленные форматы и порядок действий (SOPs) способствуют полноте передаваемой информации.

4-43. Три основных метода, используемых для предоставления

информации и разведанных:

- **Письменный.** Данный метод включают: формат (доклады в оперативной обстановке), тактические отчеты (TACREPs), или информационно-разведывательные донесения (IRs).

- **Графический.** Распространение Web-отчетов является эффективным методом для обеспечения наибольшего количества личного состава, написанной и графической информацией. Сотрудники OSINT могут сотрудничать и распространять разведывательные запросы через веб-сайты (Интернет). Информация также может быть загружена в различные базы данных для поддержки будущих операций в открытых источниках.

- **Вербальный и голосовой.** Широко распространенным способом является вербальная передача информации и разведанных, используемой во время военных брифингов. Данный метод является наиболее эффективным для информирования командиров подразделений и частей важной, секретной и своевременной информацией.

Система безопасности

4-44. Разведанные из открытых источников распространяются после проверки в системе безопасности. Данная система является приложением или набором приложений, которые проверяют информацию на подлинность и степени доступа к ней. Система также определяет общую классификацию серверов, компьютеров или сетей. Сети имеют свою систему классификации для предотвращения утраты данных.

Подразделения, занимающиеся разведкой в открытых источниках, могут обмениваться общедоступной информацией с помощью несекретных и секретных сетей в составе Сухопутных войск, а также между другими подразделениями ВС США, объединенными организациями, федеральными, государственными и местными органами власти.

4-45. Воспроизведение веб-сайтов и баз данных из несекретных сетей в секретных сетях обеспечивает разведывательный и неразведывательный персонал общедоступной информацией и открытыми источниками для поддержки объединенных наземных операций. Создание эффективной структуры ведения разведки в открытых источниках включает в себя надлежащее использование

трех основных систем безопасности:

- Объединенная глобальная система связи разведки (JWICS);
- Защищенная (секретная) распределительная сеть Интернет протокола (SIPRNET);
- Незащищенная (несекретная) распределительная сеть Интернет протокола (NIPRNET).

Объединенная глобальная система связи разведки (JWICS)

4-46. JWICS представляет собой систему взаимосвязанных компьютерных сетей, используемых различными департаментами правительства США для безопасной передачи совершенно секретной (TS) и секретной информации с особым режимом хранения (SCI) через протокол управления передачей (TCP) или Интернет протокол (IP). Данная система поддерживает синхронизацию процессов ведения разведки в открытых источниках; распространения общедоступной информации; поддержки метаданных и сотрудничества между оперативными подразделениями и подразделениями обеспечения операции.

Защищенная (секретная) распределительная сеть интернет протокола (SIPRNET)

4-47. SIPRNET также представляет собой систему взаимосвязанных компьютерных сетей, используемых различными департаментами правительства США для безопасной передачи секретной информации через протокол управления передачей (TCP) или Интернет протокол (IP). SIPRNET является основной сетью передачи данных на командно-тактическом уровне.

Данная сеть обеспечивает доступ к разведывательной информации из открытых источников через различные базы данных, а также предоставляет возможность разведывательному и не разведывательному персоналу сотрудничать, просматривать, дополнять и отслеживать изменения в требованиях разведки в открытых источниках.

Незащищенная (несекретная) распределительная сеть интернет протокола (NIPRNET)

4-48. NIPRNET используется различными правительственными ведомствами США для обмена информацией на несекретном уровне. NIPRNET предоставляет доступ к Интернету во всех подразделениях МО США. Данная сеть наиболее часто используется для проведения исследований и разведки в открытых источниках.

Факторы, влияющие процесс предоставления и распространения информации

4-49. При предоставлении и распространении данных из открытых источников, необходимо учитывать:

- **Классификация.** При анализе необработанных данных, необходимо создавать и распространять информацию на самом низком уровне секретности для распространения среди наиболее широкого количества личного состава. При написании отчетов, используйте формат «tearline» (ограничительная линия) для разделения секретной и несекретной информации для пользователей, работающих в сетях различного уровня безопасности. Организаций, установившие гриф секретности или сотрудники с производными обязанностями должны обеспечивать подведомственные организаций и персонал, руководством по классификации уровней безопасности и правилами использования информации и разведанных, полученных из открытых источников в соответствии с процедурами в документе «AR 380-5».

- **Развитие механизма обратной связи.** Электронная почта, почтовые адреса, рейтинговые системы и проведение опросов являются механизмами, которые сотрудники OSINT могут использовать для понимания информационных требования потребителя.

- **Идентификация (определение) интеллектуальной собственности.** Необходимо определять информацию, защищенную авторскими правами, запатентованной или имеющей торговую марку той или иной организации. Процесс ведения OSINT не охватывает продажу, импорт или экспорт интеллектуальной собственности. Сотрудники разведки в открытых источниках должны указывать все источники, используемые в докладе и при распространении данной информации. В случае неопределенности, сотрудники OSINT должны связаться с офисом начальника военно-юридической службы (SJA), прежде чем распространять несоответствующую информацию;

- **Использование существующих методов распространения информации** (по возможности). Создание новых методов распространения информации иногда может осложнить процесс использования уже существующих методов;

- **Аналитические сложности.** Аналитики должны понимать, что существуют трудности при составлении отчетов и распространение общедоступной разведывательной информации. Ошибки в виде заблуждения (пропуск важных сведений и прогнозы) обычно совершаются случайно, однако иногда они используются в целях убеждения или обмана. Аналитики также должны быть осведомлены о поспешных обобщениях, ложных причинах, неправильном использовании аналогов и языков, предубеждении (культурных, личных, организационных, познавательных) и оценке событий. (Более подробная информация см. ТС 2-33.4.).

ПРИЛОЖЕНИЕ А

ЗАКОНОДАТЕЛЬНЫЕ И НОРМАТИВНЫЕ ОГРАНИЧЕНИЯ

Общедоступные данные и открытые источники охватывают широкий информационный спектр. Изучение, оценка и сбор общедоступной информации может отрицательно влиять на деятельность организации, которая занимается ведением разведки в открытых источниках. В некоторых случаях, в процессе ведения разведки в открытых источниках, полученная информация может быть направлена против интересов государства, а также предоставляться самими гражданами США. Учитывая масштабы разведки в открытых источниках (OSINT) и ее эксплуатации в рамках разведывательного сообщества, необходимо обеспечить данный процесс надзором и нормативной базой со стороны разведывательного органа.

Исполнительный приказ «ЕО 12333»

А-1. Сотрудники и служащие разведывательного органа, принимающие участие во всех процессах по ведению разведки в открытых источниках должны соблюдать правовые ограничения, правила и принципы, изложенные в исполнительном приказе «ЕО 12333» и других подобных положениях, инструкциях и директивах.

А-2. В исполнительном приказе «ЕО 12333» отмечается, что основной целью национального разведывательного сообщества является обеспечение Президента и Совета национальной безопасности США необходимой информацией для содействия процессу принятия решений, касающихся развития внешней оборонной отрасли, проведения экономической политики и защиты национальных интересов страны.

А-3. Исполнительный приказ «ЕО 12333» основан на опыте операций, проводимых органом военной разведки в отношении граждан США, участвовавших в движениях по борьбе «за Гражданские права» и «Против Вьетнамской войны». Сотрудники военной разведки использовали открытые и скрытые средства для сбора информации о политических позициях граждан США, сохраняли полученные сведения в общенациональной базе данных и передавали информацию в правоохранительные органы.

А-4. В задачи исполнительного приказа «ЕО 12333» входят: расширение человеческих и технических методов сбора данных, получение сведений от иностранных спецслужб, а также осуществление эффективной борьбы и обнаружения международной террористической деятельности и шпионажа со стороны иностранных государств.

Точная и своевременная информация о возможностях, намерениях и деятельности иностранных держав, организаций и подчиненных органов необходима для принятия обоснованных военных решений руководством страны. Сбор подобной информации является приоритетной задачей, которая достигается решительным, инновационным и ответственным образом, соответствующим конституции и применимым законам и принципам США.

Толкование и применение

А-5. Устав Сухопутных войск «AR 381-10» поясняет и берет за основу исполнительный приказ «EO 12333» и директиву МО США «DOD 5240.1-R». Данный Устав позволяет разведывательному сообществу, на законном основании выполнять свои функции, при этом соблюдая конституционные права граждан США. В связи с этим, разведывательные подразделения и формирования Сухопутных войск должны иметь законные основания (приказ высшего руководства) для проведения любых разведывательных мероприятий, направленных против граждан своей страны. В соответствии с актом «the Posse Comitatus Act» (раздел 1385, глава 18, Верховный суд США), положения военного устава «AR 381-10» не относятся к разведывательным подразделениям СВ, при их участии в урегулировании гражданских беспорядков или правоохранительной деятельности без предварительного одобрения со стороны министра обороны США.

Основные функции

А-6. На основании исполнительного приказа «EO 12333», определенными функциями военной разведки США являются:

- Сбор, обработка и предоставление информации, связанной с военной деятельностью иностранных спецслужб, которая требуется для информирования министра обороны;
- Выполнение программ и миссий, необходимых для соответствия требованиям МО по предоставлению данных об иностранных государствах и спецслужбах;
- Проведение совместных мероприятий с Центральным разведывательным управлением (ЦРУ) в поддержку подразделений МО, находящихся за пределами США, а также в сотрудничестве с Федеральным бюро расследований (ФБР) в поддержку подразделений, находящихся в пределах страны. Данная процедура согласованна с министром обороны и генеральным прокурором;

- Обеспечение безопасности объектов МО, включая сферу деятельности, имущество, информацию и служащих граждан США с помощью соответствующих средств;
- Сотрудничество с соответствующими правоохранительными органами для обеспечения безопасности служащих граждан США, информации, имущества и объектов любого разведывательного органа;
- Сотрудничество с правоохранительными органами для расследования или предотвращения скрытой разведывательной деятельности со стороны иностранных государств или международных террористических организаций;
- В целях поддержки местных правоохранительных органов, осуществлять предоставление специального оборудования, технических знаний и помощи служащим гражданам США любого подразделения или агентства, а также в случаях угрозы их жизни.

Устав Сухопутных войск «AR 381-10»

А-7. Устав СВ «AR 381-10» позволяет любому подразделению СВ выполнять разведывательные функции, при этом соблюдая конституционные права граждан США. В нем также указаны рекомендации по выбору методов сбора информации, используемых для получения разведывательных и контрразведывательных данных об иностранных государствах и спецслужбах. Однако в рамках данного устава, Сухопутным войскам не дозволено вести обширную разведывательную деятельность.

Сбор информации о гражданах США

А-8. Сбор и получение информации от сотрудников спецслужб в ходе исполнения официальных обязанностей проводится с намерением использования или накопления информации для разведывательных целей. При этом необходимо основание на целевое использование собранной информации – подготовка информационно-разведывательного донесения, сообщение о происшествии (катастрофе, кризисной ситуации и т.д.), или добавления информации в общую базу данных разведывательного органа.

А-9. Для использования информации о гражданах США необходимо установление связи между сбором подобных данных и задачей разведывательного подразделения. Эта связь особенно важна при работе с общедоступной информацией, открытыми источниками и использованием информационных данных.

А-10. Субъекты военной разведки могут заниматься сбором информации о гражданах США законным путем, при этом они должны использовать наименее агрессивные методы, которые не нарушают конституционных прав сограждан (см. DOD 5240.1-R). Использование более агрессивных методов дозволено при:

- Получении информации из открытых источников или с согласия, интересующего гражданина США;
- Если доказана нецелесообразность или неэффективность получения информации от сотрудничающих источников;
- Если доказана нецелесообразность или неэффективность получения информации от других законных источников, которые не требуют ордера или разрешения генерального прокурора;
- Если доказана нецелесообразность или неэффективность отправки запроса на использование методов, требующих ордера или разрешения генерального прокурора.

А-11. Орган военной разведки может заниматься открытым сбором информации о гражданах США из иностранных источников при соблюдении следующих условий:

- Полученные из зарубежных источников разведданные носят значительный (важный) характер и не касаются деятельности гражданина США внутри страны;
- Получение разведданных из зарубежных источников не может быть достигнуто доступными методами;
- Сбор информации был согласован с ФБР в целях предотвращения нарушения хода текущих операций.

А-12. Следующие соображения применимы к сбору информации о гражданах США в сети Интернет:

- Субъекты военной разведки должны использовать правительственные компьютеры для получения доступа к сети Интернет с целью ведения служебной правительственной деятельности, если иное не разрешено;
- IP-адреса, унифицированные указатели ресурсов (ссылка - URL), а также адреса электронной почты, которые не связаны с гражданами США, могут сохраняться и обрабатываться субъектами военной разведки, без определения связи данной информации к гражданам страны, до тех пор, пока разведывательное подразделение не принимает участия в анализе, сосредоточенном на конкретных данных.

А-13. В связи с законными мерами по ограничению правительственного вмешательства в личную жизнь граждан США, закрепленных в Первой поправке к Конституции США, Устав СВ «AR 381-10» не позволяет сбор любой информации, касающейся граждан страны. Первая поправка также устанавливает, что Конгресс не имеет права издавать законов, устанавливающих создание религии и свободного ее исповедания, ограничение свободы слова, печати, права народа на проведение мирных митингов (собраний) и направления жалоб в адрес правительства.

Накопление информации о гражданах США

А-14. Хранение личной информации о гражданах США дозволено только в рамках поддержания общей базы данных, которая позволяет органу военной разведки при необходимости получить информацию о человеке с помощью запроса его имени или введения других персональных данных. Положение № 3 Устава СВ «AR 381-10» описывает виды информации о гражданах США, которые орган военной разведки может получать и хранить без согласия человека.

А-15. Устав СВ «AR 381-10» позволяет хранение информации о гражданах США в соответствии со следующими критериями:

- Информация собрана должным образом и в соответствии с положением № 2 Устава СВ «AR 381-10»;
- Орган военной разведки случайно получил информацию в соответствии с другой уполномоченной разведывательной деятельностью. Данная информация может быть сохранена если:
 - Она могла быть законно собрана в соответствии с положением № 2 Устава СВ «AR 381-10»;
 - Она необходима для понимания или оценки разведывательных или контрразведывательных данных;
 - Зарубежные разведывательные или контрразведывательные данные получены с помощью законного электронного наблюдения (РЭР).

***Примечание. Радиоэлектронная разведка (РЭР)** – это процесс приобретения сведений о частных переговорах (общении) с помощью электронных средств без согласия человека, который является участником электронного общения, или в случае неэлектронного общения, присутствующий на месте проведения общения. При этом оборудование радиопеленгации используется не только для определения местоположения*

передатчика.

- Она связана с проводимым сбором данных и может указывать на деятельность, нарушающую федеральные, государственные, местные или международные законы.

- Информация относится к функциям и обязанностям других видов деятельности СВ, компонентов МО или не военных агентств, а также используется только для передачи данной информации, соответствующему учреждению. Переданные данные подлежат сбору и последующему уничтожению в соответствии с основными функциями делопроизводства. При этом подразделение военной разведки не должно сохранять данную информацию в разведывательных базах данных и других хранилищах.

А-16. Временная задержка. Подразделения военной разведки имеют право временно (до 90 дней) задерживать передачу данных о гражданах США с целью установления оснований на законное хранение подобной информации в соответствии с Уставом СВ «AR 381-10». Отсчет времени (90 дней) начинается с момента получения информации.

А-17. Другая информация, находящаяся в наличии подразделения военной разведки должна быть предоставлена вышестоящему руководству для ее учета и дальнейшего рассмотрения.

А-18. Доступ к информации о гражданах США, хранящейся в разведывательных документах, базах данных и других хранилищах, имеют только сотрудники, деятельность которых выявляет необходимость в ознакомлении с подобной информацией.

Информация о гражданах США хранится в форме разведывательных документов, базы данных и других хранилищ в соответствии с правилами Системы управления делопроизводством Сухопутных войск «AR 25-400-2». Подразделения военной разведки ежегодно обязаны проводить проверку разведывательных документов и баз данных, а также отдельно рассмотреть соответствие исполнительным функциям и необходимость дальнейшего хранения информации о гражданах США. Это гарантирует, что данная информация не хранится в нарушении, установленного свода правил. Данные инструкции не относятся к «Архиву следственной документации» или другим хранилищам с длительным сроком хранения данных.

Распространение информации о гражданах США

А-19. Распространение данных – это процесс управления информацией,

в ходе которого соответствующие сведения (любого характера) передаются в доступной форме от одного человека или места в другое.

Данный процесс осуществляется с помощью различных средств с целью улучшения понимания обстановки, а также для инициирования или руководства действиями (см. FM 6-0). Другими словами, распространение данных является процессом информирования пользователей разведывательной информацией о соответствующих миссиях, задачах и функциях. Положение № 4 Устава СВ «AR 381-10» определяет виды информации о гражданах США, которые орган военной разведки может распространять без согласия вовлеченного объекта за пределы подразделения, которое получило соответствующую информацию.

Сомнительная разведывательная деятельность

A-20. Сомнительная разведывательная деятельность происходит, когда разведывательные операции потенциально нарушают:

- Законы;
- Исполнительные приказы;
- Директивы президента;
- Нормативные принципы МО и СВ.

A-21. В соответствии с Уставом СВ «AR 381-10», сотрудники разведывательного органа должны сообщать о сомнительной разведывательной деятельности вышестоящему начальству, главному инспектору или напрямую заместителю министра обороны по вопросам разведки. Ниже приведены примеры сомнительной разведывательной деятельности по неправомерному сбору, сохранению и распространению информации о гражданах США:

- Сбор и получение информации об американских организациях, не связанных с деятельностью иностранного государства или международной террористической группировки;
- Подготовка и распространение разведывательных прогнозов об угрозах, содержащих информацию о гражданах США, без четкого объяснения цели мероприятий для которой данная информация была собрана;
- Сбор и накопление информации о гражданах США в целях защиты

войск без определения законности данной разведывательной функции;

- Сбор и накопление информации о гражданах США из открытых источников без логической связи к миссии (задаче) подразделения.

А-22. Устав СВ «AR 381-10» направляет разведывательные подразделения на согласование вопросов, касающихся толкования инструкции по сбору, хранению и распространению информации о гражданах США, к начальникам юридической службы штаба своего подразделения.

Заместитель помощника Директора национальной разведки в открытых источниках

А-23. В обязанности заместителя помощника директора национальной разведки в открытых источниках (ADDNI / OS) входят:

- Осуществление интеграции, оценки и надзора за деятельностью Национального предприятия разведки в открытых источниках (NOSE);

- Обеспечение контроля и руководства за ведением разведки в открытых источниках на стратегическом уровне;

- Осуществлять председательство в Национальном комитете по открытым источникам (NOSC) и Комиссии советников по открытым источникам;

- Осуществление надзора за Центром открытых источников при директоре национальной разведки (DNI OSC) и подчиненными организациями Национального предприятия разведки в открытых источниках (NOSE);

- Обеспечение интеграции стратегии управления процессом сбора информации из открытых источников;

- Разработка порядка руководства Национальным предприятием разведки в открытых источниках (NOSE);

- Установление контроля над процессом межведомственного обмена информации из открытых источников.

Разведывательное сообщество

А-24. В обязанности разведывательного сообщества входят:

- Разработка программного контроля и оценки под централизованным руководством ADDNI / OS;

- Поддержка всех разведывательных дисциплин;

- Создание соответствующего порядка проверки надежности источников

и информации;

- Разработка системы оценки общей деятельности в открытых источниках;
- Предоставление доступа разведывательному сообществу ко всем базам данных общедоступной информации и услугам.

Национальный комитет по открытым источникам (NOSC)

A-25.NOSC обеспечивает руководство Национального предприятия разведки в открытых источниках (NOSE). В обязанности NOSC входят:

- Разработка соответствующих стандартов для проверки надежности источника и информации, конспирации и обучения;
- Развития научно-технических стандартов для хранения метаданных.

Директор национальной разведки Центра открытых источников (DNI OSC)

A-26.Основной целью DNI OSC является модернизация процесса использования открытых источников путем приобретения, обмена, анализа и распространения информации и услуг. В обязанности DNI OSC входят:

- Оказание содействия партнерам и клиентам правительства США в эксплуатации открытых источников;
- Обеспечение безопасности соответствующих лицензионных соглашений с пользователями открытых источников;
- Разработка программ для эффективного использования открытых источников;
- Обучение и подготовка сотрудников для правильного использования информации из открытых источников в соответствии с системой безопасности.

ПРИЛОЖЕНИЕ В

ОСВЕДОМЛЕННОСТЬ ПО ВОПРОСУ КИБЕРБЕЗОПАСНОСТИ

Сотрудники разведки, осуществляющие сбор информации в открытых источниках, должны понимать оперативную обстановку в сети Интернет, минимизировать и снижать оставление кибер «следов», эффективно применять методы кибербезопасности, использовать безопасный интернет-серфинг и понимать, что в документах могут содержаться встроенные метаданные.

Ситуационная осведомленность о киберпространстве и кибербезопасности

В-1. Ведение разведки в открытых источниках больше чем любой другой вид разведывательной деятельности может непреднамеренно раскрыть содержание требований к информации, необходимой командиру (CCIRs). Для

проведения исследований в открытых источниках иногда требуется доступ к веб-сайтам с расширением .mil или .gov, доступ к которым иногда заблокирован. Знания о безопасном использовании Интернет-ресурсов необходимы для эффективного, агрессивного и успешного проведения разведки в открытых источниках. Необоснованное ограничение доступа к Интернету может серьезно препятствовать процессам сбора, обработки, подготовки справок и распространения общедоступной информации из открытых источников.

В-2. Осведомленность начинается с эффективной кибербезопасности. Необходимо помнить, что при осуществлении поиска в Интернете компьютеры автоматически передают такие характеристики, как операционная система, версия каждой встроенной программы, уровни безопасности, историю посещения веб-сайтов, спамы, предпочтение пользователя, IP адрес, поддержка языков и URL ссылки. На основе критерий поиска, местоположения, языка и времени посетители часто перенаправляются на другие веб-сайты.

В-3. В связи с сотнями тысяч взаимосвязанных сетей, состоящих из миллионов компьютеров, сеть Интернет носит название «сеть сетей». Компьютеры и пользователи, подключенные к сети Интернет, идентифицируются по конкретной системе IP-адреса, который определяет его местоположение. IP-адрес служит адресом, по которому передается информация. Основной угрозой является посещение небезопасных и сомнительных веб-сайтов в рабочее время, что может непреднамеренно раскрыть деятельность подразделения.

Озабоченность в нем лежит в понимании того, что во время посещения нестандартных или сомнительных интернет веб-сайтов в соответствии со служебными обязанностями, конфиденциальной информации устройство может быть обнаружено случайно.

В-4. В рамках информационной среды киберпространство является глобальной сетью и состоит из взаимозависимых сетей информационно-технологической инфраструктуры: Интернет ресурсов, телекоммуникационные сети, компьютерные системы, встроенные процессоры. Сухопутные войска активно используют возможности киберпространства, в качестве целостной и неотъемлемой части проведения наземной операции. В целях эффективного ситуационного информирования о

кибер-угрозах, сотрудники, проводящую разведку в открытых источниках, должны понимать среду киберпространства.

В-5. В результате осуществления разведывательной деятельности в киберпространстве и получении дружественной, нейтральной и предупреждающей информации поддерживается ситуационная осведомленность о киберпространстве.

Она достигается в результате:

- выявления угроз, с целью дальнейшего определения их влияния на проведение операции дружественными силами и принятие своевременных контрмер;

- определения порядка эффективного использования киберпространства, с целью получения поддержки со стороны дружественных и нейтральных лиц;

- определения порядка получения, поддержания и использования технических и операционных преимуществ.

В-6. При активном взаимодействии с веб-сайтами появляются угрозы, оказывающее негативное влияние на безопасное проведение операции и защиту компьютера. Оставляя «цифровые следы» на страницах веб-сайтов, осуществление поиска в сети Интернет может поставить под угрозу безопасность операции. Осуществление «серфинга» в сети Интернет, может поставить под угрозу компьютерную безопасность и допустить случаи проникновения вредоносных программ (вирусы, черви и троянские кони) или несанкционированного доступа. Для определения потенциальных угроз, сотрудники разведывательного органа должен быть бдительным, использовать только разрешенное оборудование и программного обеспечение, а также соблюдать установленные правила обеспечения безопасности.

В-7. При посещении сайта сотрудниками разведывательных подразделений в сети Интернет остаются ссылки на посещенные ими сайты, что может поставить под угрозу компьютерную безопасность и раскрыть технические данные и интересы подразделения.

Пример информационной кибербезопасности

Если пользователь вводит в поисковик: Брэдли армия США, первая URL ссылка в поисковике «Google» будет следующей:

<http://www.google.com/search?hl=en&q=bradley+us+army>. Эта ссылка поможет определить сайты, которые посетил пользователь для осуществления поиска

информации на английском языке о генерале армии Н. Омаре Брэдли и американской боевой машине пехоты Брэдли.

В-8. Все нижеперечисленные действия пользователя, которые осуществляются на веб-сайтах, автоматически регистрируются и сохраняются в виде информации, которая называется «cookie».

- введенные для поиска слова;
- результаты поиска;
- кнопки-выбора;
- осуществленные действия на веб-сайте (изменение домена или адреса).

В-9. На многих веб-сайтах, информация, которую пользователь предоставляет или заполняет, автоматически становится частью веб-сайта и доступным при поиске другими лицами. Важные информации, требующие ограничение доступа:

- военные планы;
- военные операций;
- военные учения;
- карты и схемы;
- места дислокации;
- расписания;
- уязвимости военной техники и возможностей, недостатки;
- имена и их номера;
- телефонные номера;
- даты рождения;
- идентификационные номера.

В-10. Традиционные и нетрадиционные угрозы имеют разрушительный характер и активно используют киберпространство для проведения кибер-атак против армии США.

Кибер-угрозы включают в себя инновационные, сетевые и технологически продвинутые характеристики.

Противники, в целях создания и поддержания своих структурных и общественных преимуществ в интересующих их областях, таких как управление операцией, увеличение личного состава, логистика, информационное воздействие, пропаганда, сбор и отмывание денег, активно используют новые технологии.

В-11. При осуществлении разведки в открытых источниках с использованием компьютерных систем и сети Интернет, необходимо оценить уязвимость сетей, угрозы безопасности (физические и виртуальные) и ожидаемые риски.

ПРИЛОЖЕНИЕ С

ОСНОВНЫЕ И ПРОДВИНУТЫЕ МЕТОДЫ ПОИСКА В ИНТЕРНЕТЕ

Возможность осуществления поиска в Интернете является важным навыком при ведении разведки в открытых источниках. Интернет рассматривается, как средство ведения разведки, наблюдения и

Исследовательский Центр Виктора Воксанаева
Бюллетень OSINT № 33 (сентябрь – октябрь 2013 г.)

исследования, обеспечивает доступ к веб-сайтам и базам данных, которые содержат широкий спектр информации о местах проведения текущих, планируемых и потенциальных военных операций. В результате прогресса в области компьютерных технологий и сети Интернет, в настоящее время военнослужащие, как никогда прежде, имеют широкий доступ к большому количеству общедоступной информации и огромные возможности по их обработке. Совокупность сведений о культуре, экономике, географии, военном деле и политике, которая в прошлом в некоторой степени была недоступна для общественности, в настоящее время находится на руках у учеников средней школы и студентов, которые в будущем станут руководителями вооруженных сил.

Всемирная паутина и DEEP WEB

С-1. Интернет представляет собой динамичную информационную среду, состоящую из неподвижных и движущихся виртуальных и специальных веб-сайтов, содержащих смесь старых и новых информации. Существует множество виртуальных баз данных, которые увеличиваются с геометрической прогрессией. Двигаясь в ногу с новыми технологиями, сотрудники, занимающиеся разведкой в открытых источниках, могут противостоять любым проблемам.

Всемирная паутина (интернет пространство)

С-2. WWW индексируется по стандартным информационно-поисковым системам. Стандартные информационно-поисковые системы, как правило, неспособны получить доступ или завладеть информацией, необходимой для эффективного проведения разведки в открытых источниках. Общий объем информации в сети Интернет составляет более 7,5 тыс. терабайтов и продолжает увеличиваться. При использовании обычных информационно-поисковых систем можно найти только одну четверть всей необходимой информации. Считается, что при ведении разведки в открытых источниках из всего объема информации, находящейся в сети Интернет, можно увидеть лишь ее часть. Остальные три четверти (или примерно 5,6 тыс. терабайтов) содержатся в так называемом Deep Web.

DEEP WEB

С-3. Deep Web не является частью традиционной всемирной паутины и содержит в два раза больше информации. В отличие от всемирной паутины,

Deep Web не индексируется. Веб-сайты и базы данных, расположенные на нем не доступны при осуществлении поиска через традиционные поисковые системы. Deep Web предлагает огромное количество ресурсов следующего содержания:

- динамического. Веб-страницы, появляющиеся при осуществлении поиска;
- ответ на представленный запрос;
- несвязанного. Веб-страницы, которые не связаны с другими веб-страницами и блокирующие доступ к своему содержанию при использовании стандартных программ поиска информации;
- скрытого. Веб-страницы без обратных и входящих ссылок;
- ограниченного доступа. Веб-сайты, которые ограничивают доступ к информации;
- не имеющие гипертекст. Текстовое содержание закодированное в формате мультимедийных файлов, которые не обнаруживаются поисковыми системами.

Поисковые системы

С-4. Поисковые системы являются основными инструментами, которые используют сотрудники OSINT при проведении разведки и сбора общедоступной информации из открытых источников. Сотрудники OSINT активно используют поисковые системы и разные критерий поиска, чтобы найти текст, изображение и информацию на страницах тысячи веб-сайтов. Технически, поисковые системы осуществляют поиск по индексу веб-сайтов. Коммерческие и государственные поисковики отличаются друг от друга в зависимости от параметров поиска, осуществления процесса поиска и способами предоставления результатов поиска. Большинство поисковых систем используют так называемые программы-сборщики, которые могут построить индексируемые базы данных. Программы-сборщики осуществляют поиск в Интернет веб-сайтах и автоматически сохраняют найденные файлы в своей базе данных.

С-5. Большинство поисковых систем при отображении результатов поиска используют формулу релевантности (в первую очередь показывают важную информацию, расположенную в определенном порядке, с кратким описанием и ссылкой на нее).

Это помогает определить, насколько хорошо ответ соответствует запросу.

С продолжающимся развитием поисковых систем, формула релевантности имеет большое значение, так как она не показывает одинаковые результаты. Размещение ключевых слов дает разные результаты, если переставить в связи с более акцентом на одно слово за другим. С развитием методов поиска, некоторые поисковые системы начали более эффективно находить конкретные виды информации, такие как статистические и финансовые данные и новости. Для увеличения результативности, программные инженеры разработали метапоисковики, которые позволяют пользователю осуществлять поиск информации на нескольких системах одновременно.

Поисковые системы

В случае если определенная поисковая система не может вместить фразы в кавычки или преобразовать запрос в другие виды булевых функций (*логическая функция; Булевы функции названы в честь английского математика XIX века Дж. Буля, который впервые применил алгебраические методы для решения логических задач*), то метапоисковик исключает заданные параметры из поиска.

Результатом такого поиска станет предоставление общей информации, которая будет менее эффективной по сравнению с хорошо отформатированным поиском в специализированных поисковых системах, позволяющих находить более детальную информацию.

С-6. Сотрудники спецслужб, понимая механизм работы поисковых систем:

- проводят первоначальные поиски с использованием ключевых слов и сочетаний;
- для улучшения параметров поиска активно применяют булеву функцию;
- проводят последующие поиски с использованием естественного языка.

ПОИСК ПО КЛЮЧЕВЫМ СЛОВАМ

С-7. При осуществлении поиска по ключевым словам, сотрудники OSINT должны определить какие слова являются уникальными (ключевыми) в необходимой для них информации.

Во избежание иррелевантной (ненужной) информации и получения соответствующих результатов, применение ключевых слов должно быть сбалансированным.

Общие слова (английского языка), которые следует избегать:

- неопределенный артикль *A*;
- неопределенный артикль *An*;

- союз *And*;
- определенный артикль *The*.

С-8. При осуществлении поиска в сети Интернет, в целях получения эффективного результата, необходимо уменьшить использование вышеперечисленных слов, за исключением, когда они являются частью названия статьи или книги. Большинство поисковых систем игнорируют общие слова. Например, если искать информацию о продаже русских и китайских танков в Ираке, не нужно использовать слово танк в роли ключевого слова. Вместо этого, используйте дополнительные определяющие слова, такие как «Продажа Российских или Китайских танков в Ираке».

Логические операторы (булева функция), контроллеры и разделители данных

С-9. При осуществлении поиска в соответствии с правилами компьютерных поисковиков, можно найти подавляющее большинство необходимых данных. Логическую связь между критериями поиска называют булевой логикой. Этот метод поиска предоставляет возможности для построения логических связей между критериями поиска с использованием местных операторов, контроллеров и разделителей данных.

С-10. Логические операторы, контроллеры и разделители помогают сотрудникам спецслужб при установлении связей между словами, необходимой для повышения эффективности поиска.

Пример использования логических операторов

Поисковая система осуществляет поиск информации со словами «русский» и «танк», а при размещении их в скобках, например, (русский танк) и для исключения из результатов поиска информации о китайских танках, при поиске о продажах в Ираке используйте словосочетание (русский танк), НЕ (китайский танк).

Сотрудники могут также использовать функцию поиска «NEAR», когда отношения и расстояние между терминами хорошо известны. Например, если сотрудники разведки ищут случаи продажи танка в Багдаде, то мы знаем, что новостные статьи размещают название места нахождения в своем названии из, как обычно, пяти слов или содержания. Поэтому можно использовать функцию «NEAR / 5» для поиска информации о продаже танка.

Таблица С-1. Логические операторы (булева функция), контроллеры и разделители данных

Функции	Булева функция	Пример
Должно включать *	AND	Химический AND оружие Химический * оружие
Не должно включать	NOT	Африка NOT Судан
Может включать	OR	Химический OR биологический
Законченная фраза	* *	*Продажа Ираку китайского танка*
Вложенные	()	(Светлый путь)
Приблизительные**	NEAR	«Белый дом» NEAR «воздушное вторжение»
Шаблоны	Слово* или *слово	Оружие * (порох)

Примечание. Булевы поиски могут не работать на всех поисковых системах. Можете использовать опцию «Расширенный поиск», которая доступна на многих веб-браузерах. При расширенном поиске необходимо заполнить такие поля, как «Поиск в веб-страницах, которые содержат все эти слова, этой точной формулировки или фразы» или «не показывать страницы, включающие любое из этих слов».

Поиск на естественном языке

С-11. Альтернативным способом поиска является осуществление поиска в формате вопросов на естественном языке, поскольку большинство крупных поисковых систем включают в себя данную функцию. Если при поиске вопрос содержит все необходимые слова, сотрудники OSINT получают наилучшие результаты. Одним из основных недостатков этого метода является то, что он выдает большое количество результатов, на анализ которых потребуется много времени. Если необходимая информация отсутствует на первой странице результатов поиска, то вопрос должен быть уточнен, чтобы возобновить поиск с использованием других параметров.

Веб-сайты сети Интернет

С-12. Существуют четыре шага предназначенные для эффективного

использования общедоступной информации и открытых источников:

- составление плана поиска в Интернете;
- осуществление поиска в Интернете;
- уточнение параметров поиска в Интернете;
- сохранение результатов поиска.

План поиска в сети Интернет

С-13. Сотрудники OSINT для составления плана поиска должны понять информационно-разведывательные требования, которые помогут определить виды необходимой информации, места их поиска, а также предоставят ключевые слова, используемые при осуществлении поиска. После определения направленности и ключевых слов, Сотрудники OSINT используют интернет-браузеры и поисковые системы для подключения к ранее выявленным сайтам.

Поиск по ключевым словам

Если подразделение планирует провести операцию по оказанию гуманитарной помощи в той или иной стране, задачей разведывательных органов будет определение мест концентрации беженцев этой стране. Задачей сотрудников, ведущих разведку в открытых источниках, будет определение:

- Организации по оказанию гуманитарной помощи, руководящие работой центров распределения продовольствия;
- Центров сосредоточения населения;
- Мест скопления ополченцев;
- Мест оперирования ополченцев за последние 30 дней.

Некоторые полезные параметры поиска:

- беженцев;
- оказание гуманитарной помощи;
- ополченцы;
- источники пресной воды.
- места продажи продовольственных товаров.

Определение мест, где беженцы могут или не могут находиться:

- центры-помощи неправительственных организаций;
- места питания;
- источники вода;
- Враждебные силы ополченцев. На основе требований разведки, главной

целью поиска в Интернете является определение мест скопления беженцев в

стране.

Порядок осуществления поиска в сети Интернет

C-14. В целях исследования интересующего вопроса, сотрудники OSINT при помощи соответствующих запросов проводят первоначальный поиск вероятных источников информации. Первоначальный поиск является первым из всех последующих поисков данных и информации, которые получены и зарегистрированы в соответствии с планом исследования.

Полученная информация автоматически интегрируется в соответствующие цифровые или аналоговые базы данных. Сотрудники OSINT должны избегать искушения использовать только одну поисковую систему, поскольку каждая имеет свои сильные и слабые стороны. Организационные стандарты, опыт исследований и экспертные рекомендации, обычно подсказывают какую поисковую систему необходимо использовать.

Примечание. Если в течение 30 минут поисковые системы не могут обнаружить необходимую информацию, то вполне возможно, что данная информация не существует в Интернете, не была проиндексирована или имеет безвозвратный формат.

Повышение эффективности поиска в Интернете

C-15. первые несколько страниц результатов поиска, как правило, являются наиболее актуальными.

Основываясь на этих страницах, сотрудники OSINT анализируют первые результаты поиска на предмет важности и точности, с целью определения их соответствия разведывательным требованиям, а в случае необходимости возобновления поиска.

Результаты первоначального поиска в Интернете могут быть недостаточны, чтобы удовлетворить информационно-разведывательные требования. Сотрудник OSINT обычно используют следующие методы улучшения результатов поиска:

- изменение порядка и критериев поиска;
- изменение правописания и грамматики;
- регулировка верхнего или нижнего регистра;
- использование другие варианты ключевых слов;
- поиск в результатах;
- поиск по колонкам;

- поиск в кэш-памяти и архиве;
- усечение URL;
- домены веб-сайтов.

Изменение условий поиска

C-16. Поисковые системы могут уделить больше внимания на значение первого или одного слова во фразе поисковой строки. Например, изменение порядка слов (devices explosive to explosive devices; взрывное устройство на устройства взрыва) может выдать различные результаты поиска.

Изменение орфографии и грамматики

C-17. Поисковые системы пытаются подобрать точное написание слова в строку поиска. Существуют поисковые системы, которые распознают альтернативные варианты и предлагают их, чтобы пользователь мог исправить общие ошибки в слове или в предложении. Например, изменение написания слова American-English center на the British-English centre может привести к разным результатам. Булева логика также может быть использована для того, чтобы избежать возможных ошибок в правописании. Кроме того, изменение правописания транслитерированного названия образует разные результаты, которые могут быть полезны в зависимости от целей поиска. Например:

- Al-Qaeda (Аль-Каеда);
- al-Qaida (аль-Каида);
- al-Qa'ida(аль-Кайеда);
- el-Qaida (ель-Каида);
- al Qaeda (аль Каида).

Установление строчных и заглавных букв

C-18. Функции некоторых поисковых систем не предусматривает распознавание размера букв. Они подбирают именно такие слова, какие указаны в параметре поиска. У большинства систем при осуществлении поиска все буквы должны быть строчными.

При поиске имени человека, географического положения, названия или других слов имеющих заглавную букву, необходимо использовать поисковую систему с учетом регистра. Например, изменение написания таких слова, как java и JAVA выдает разные результаты.

Использование ключевых слов

C-19. Сотрудники OSINT используют термины, которые являются культурно и географически распространенными. Использование других вариантов ключевых слов может улучшить результаты поиска (например: полицейский, коп, жандарм, карабинер и т.д).

Поиск в результатах

C-20. Если первоначальный или последующий поиск предоставляет хорошие, но все еще неудовлетворительные результаты, сотрудники OSINT, в целях увеличения вероятности обнаружения необходимой информации, могут возобновить поиски в уже найденных материалах. Большинство поисковых систем, чтобы помочь пользователю, отображают такие опции, как поиск в найденных материалах или на похожих страницах.

Поиск по группам

C-21. При осуществлении поиска по группам, в отличие от поиска в Интернете, сотрудники OSINT ищут ключевые слова в унифицированных указателях ресурсов. Обычно это делается, когда поисковик в результате поиска показывает большое количество ссылок на информации. Существует много систем, осуществляющих поиск по группам, каждая из которых имеет свои сильные стороны:

- по важности. Выполняет поиск веб-сайтов с определенной гиперссылкой;
- по домену. Выполняет поиск конкретных доменов;
- по сходству. Выполняет поиск аналогичных или связанных с какой-либо ссылкой веб-сайты;
- по ссылке. Выполняет поиск конкретных гиперссылок, встроенных в веб-сайты;
- по тексту. Выполняет поиск определенного текста в содержании веб-сайта;
- по URL-адресу. Выполняет поиск определенного текста в полном адресе веб-сайта.

Поиск в кэш-памяти и архиве

C-22. Иногда в результате поиска мы получаем ссылку на интересующую нас информацию, но при попытке открыть его, веб-сайт временно не работает. В таких случаях, если поисковая система записывает данные и определяет URL-адрес, выберите ссылку в кэш-памяти, чтобы получить

доступ к исходным данным. Сотрудники OSINT также могут найти его содержание на таких сайтах, как www.archive.org. Сотрудники OSINT должны понимать, что такая информация является старым и не обновлялась создателями сайта.

Усечение URL

С-23. Основываясь на теме информационно-разведывательных требований, сотрудники OSINT могут вручную осуществлять поиск среди полученных результатов путем усечения URL к веб-сайту.

OSINT персонала работать в обратном направлении от первоначального результата поиска на веб-сайт, содержащий нужную информацию или базу данных, удалив в конце сегменты URL на косую черту. См. ручную обрыва URL Например, в таблице С-2.

С-24. Также существуют сайты сокращения URL-адреса, которые перенаправляют пользователя с коротким URL-адресом на более полный URL-адрес, выступающий в качестве официального адреса веб-сайта. Данный метод часто используется в социальных сетях, таких как Twitter.

Таблица С-2. Усечение URL-адреса

Усечение URL-адреса вручную	
Пример	http://www.website.com/default.aspx?utm_source=twitter&utm_medium=social-media
Удалить все, но оставить основную часть сайта	http://www.website.com/
Усечение URL с помощью сайта	
Пример	http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353259562_2?pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79T370AM3&pf_rd_t=201&pf_rd_p=1270985982&pf_rd_i=B00

	2Y27P3M
Веб-сайт, изменяющий формат URL-адреса, производит копию данного адреса для использования в настройках социальных сетей или в электронной почте.	http://tinyurl.com/KindleWireless

Домены веб-сайтов

С-25. Доменные имена в сети Интернет выявляют ярлыки и используются в различных контекстах компьютерных сетей. Они выступают в качестве простых ярлыков идентификации права владения или контроля над информационными ресурсами. В результате существования миллионов URL-адресов в сети Интернет, сотрудники спецслужб сталкиваются с множеством веб-сайтов, которые могут или не могут предоставлять и содержать информацию, представленную в данном домене.

Домены, перечисленные в таблице С-3, надежны, так как они управляются на государственном уровне и написаны этими организациями.

Примечание. Сотрудники OSINT, использующие общедоступную информацию из открытых источников с расширением *org*, *info* или *net* не должны принимать их в качестве надежных сайтов, потому что домены данных сайтов могут быть созданы недобросовестными организациями.

Таблица С-3. Распространенные домены веб-сайтов

Домен	Описание
.aero	Предназначено для членов авиатранспортной отрасли
.biz	Только для бизнеса
.com	Неограниченный домен верхнего уровня, предназначенный для коммерческого содержания
.coop	Предназначено для кооперативных объединений
.edu	Предназначено для высших учебных заведений, аккредитованных агентств из списка департамента образования США
.gov	Предназначено только для правительства США

.info	Неограниченный домен верхнего уровня
.int	Используется только организациями, образованными в результате международного договора между правительствами
.jobs	Предназначено для менеджеров человеческими ресурсами
.mil	Исключительно для военнослужащих США
.museum	Предназначено для музеев
.name	Предназначено для физических лиц
.net	Предназначено для объединения технологических лиц
.org	Предназначено для некоммерческого использования, но открыты для всех пользователей сети Интернет
.pro	Только для аккредитованных профессионалов и связанных с ними лиц

Базы данных, программное обеспечение и инструменты открытых источников

C-26. Существуют множество приложений коммерческих программ, инструменты и базы данных, которые для осуществления поиска используют слова запроса. Существуют следующие поисковые системы:

- **Академия Google**. Академия Google предоставляет простые способы обширного поиска научной литературы.

Данная система поиска может из одного места осуществлять поиск во всех существующих дисциплинах и источниках, содержащие в себе статьи, диссертации, книги, рефераты. Академия Google помогает пользователю найти необходимую для него работу из всех доступных мировых научных исследований.

- **Spokeo**. Специализируется на сборе информации о людях (*их имена, адреса, номера телефонов*) из телефонных книг, социальных сетей, маркетинговых списков, бизнес-сайтов и других открытых источников. При осуществлении сбора данных в логически последовательные профили, Spokeo использует алгоритмы.

- **Blog Pulse**. Представляет собой автоматизированную систему определения тенденции в блогах путем применения компьютерного обучения и методов обработки естественного языка.

- **Pipl**. Система запросов помогает найти Deep Web, которые не могут

быть найдены при поиске стандартными поисковыми системами.

Piñ использует передовые алгоритмы анализа языка и классифицирования для получения самой актуальной информации об интересующей разведку личности.

- **Monitter**. Поисковая система, созданная на основе браузера Twitter. Monitter отображает в вашем браузере сразу три постоянно обновляющихся поисковиков по ключевым словам.

- **Maltego**. Данная система является аналитическим приложением, которое предоставляет сбор и анализ данных, а также формирование смысловых группировок полученных сведений. Maltego позволяет определить существующие ключевые связи между информацией, а также выявить ранее неизвестные.

Инструменты Google

C-27. Инструменты Google оказывают помощь при использовании общедоступной информации из открытых источников:

- запросы;
- типы запросов;
- модификатор запросов.

Запросы

C-28. Google поддерживает ряд продвинутых логических операторов, запросы которых имеют особое значение для Google. Обычно, при применении операторами разных типов и модификаторов запросов, изменяются параметры и результаты поисковых систем.

Типы запросов

C-29. Существует четыре категории запросов, охватывающих большинство веб-запросов:

- **Кэш-память**. Если другие слова включены в запрос, то Google выделяет эти слова в кэшированных документах. Например, [Кэш: www.google.com веб] показывает, что сохраненное в кэш-содержание с выделенным словом веб.

- **Ссылка**. Запрос [ссылка:] показывает списки веб-страниц, которые ссылаются на определенную веб-страницу. Например, [ссылка: www.google.com] показывает веб-страницы, которые имеют ссылки на домашнюю страницу Google.

- **Связанные**. Запрос [связанные:] показывает списки веб-страниц, которые похожи на определенную веб-страницу. Например, [связанные:

www.google.com] выдает списки веб-страниц, которые похожи на домашнюю страницу Google.

- **Информация.** Запрос [информация:] предоставляет некоторую информацию об определенной веб-странице из архива Google. Например, при запросе [информация: www.google.com] отображается информация о главной странице Google.

Модификаторы запросов

C-30. Исследования с использованием определенного поискового запроса можно изменить с помощью следующих модификаторов:

- **сайт.** Если слово [сайт:] включен в запрос, то поиск будет ограничен и осуществляться только на веб-сайте указанного домена.

Например, такой запрос как [*помощь* сайт: www.google.com] находит информацию о *помощи* только на страницах www.google.com., [*помощь* сайт: com] находит информацию о помощи только в унифицированных указателях ресурса *com*.

- **Allintitle** (все в названии). Если запрос начинается со слова [allintitle:], то результаты будут ограничены, поиск будет осуществляться только на тех веб-сайтах, у которых запрашиваемое слова является включено в название сайта. Запрос [allintitle: Google и поиск] показывает только такие документы, которые в своем названии имеют слова *Google* и *поиск*.

- **Intitle** (в названии). Если слово [intitle:] включено в запрос, то результаты будут ограничены документами, которые содержат это слово в своем названии. Например, [intitle: Google Search] показывает документы, которые содержат слово *Google* в своем названии и содержат второе слово *Search* в любом месте документа (не обязательно в названии).

Размещая [intitle:] перед каждым словом запроса покажет такие же результаты если в используете модификатор [allintitle:]. Например, результаты запроса [intitle: Google intitle: Search] будут одинаковы с результатами запроса [allintitle: Google Search].

- **Allinurl** (все в URL). Если запрос начинается со слов [allinurl:], то поиск будет осуществляться только на тех веб-сайтах, которые имеют запрашиваемое слово в URL. Например, такой запрос [allinurl: Google Search] показывает только те документы, которые имеют слова *Google* и *Search* в URL.

- **Inurl** (в URL). Если слово [Inurl:] включено в запрос, то результаты ограничиваются теми документами, которые имеют запрашиваемое слово в

содержании в URL. Например, запрос [Inurl: Google Search] показывает только те документы, которые содержат слово Google в их URL-адресе, а слово Search в любом месте документа (в URL или нет). Ввод «Inurl:» перед каждым словом запроса равносильно вводу «allinurl:» в передней части запроса. Например, результаты запросов [Inurl: Google Inurl: Search] и [allinurl: Google Search] будут одинаковы.

Международные сайты в сети Интернет

Число зарубежных пользователей всемирной паутины и Deep Web все чаще превосходят англоговорящего пользователя. Этот получается в результате создания иностранных веб-сайтов с определенными кодами стран. Сотрудники OSINT должны знать историю происхождения иностранных веб-сайтов и их потенциальных уязвимых мест.

Факторы, влияющие на методы сбора информации в Интернете

C-31. При проведении простого и расширенного поисков в сети Интернет, техника областей, необходимо рассмотреть следующие технические области:

- **программное обеспечение COTS.** При использовании инструментов и программного обеспечения COTS, сотрудники OSINT должны знать, что инструменты и программное обеспечение необходимо использовать в соответствии с руководящими документами и политике.

- **создание каталогов и архивов.** В связи с природой интернет-сайтов и отсутствием контроля, веб-сайты могут быть удалены из всемирной сети Интернет без предварительного уведомления.

- **авторство.** Часто, авторами общедоступных материалов могут быть неизвестные люди.

- **выявленные веб-сайты и порталы.** Ознакомление с общедоступной информацией обычно приводит к стандартизации веб-сайтов и порталов, используемых для исследований.

Веб-сайты и порталы, носят субъективный характер из-за предубеждений и представлений об их администраторе или дизайнере.

- **автономные браузеры.** В связи с нестабильностью и непредсказуемостью веб-сайтов, эффективное использование автономных браузеров может улучшить исследования в сети Интернет.

Уязвимые места сети Интернет и разведки в открытых источниках

C-32. Основной целью OSINT является использование общедоступной информации из открытых источников, не раскрывая сведений о своих

сотрудниках или организации. Процесс использования общедоступной информации из открытых источников, как правило, является анонимным и уменьшает риски потенциального раскрытия безопасности военной операции. При проведении исследований в сети интернет и Deep Web существуют неминуемые угрозы. Ведение разведки в открытых источниках может поставить под угрозу безопасность операции и раскрыть информацию о пользователе (сотруднике разведки США) и через IP-адрес выдать местоположение его компьютерных систем. Любое количество инструментов разрушения компьютерных системы может сделать процесс ведения разведки в открытых источниках неэффективным. Они включают в себя:

- **вирусы**. Компьютерные коды, которые подключаются к компьютерным программам. После присоединения, вирусы заражают другие компьютеры через репликацию (самокопирование).

- **тройанские кони**. Компьютерные программы, которые мешают пользователю активировать команды.

- **черви**. Автономные компьютерные программы, которые заражают компьютеры через самокопирование. Черви создают трафик на веб-сайтах с целью уменьшения видимости путем проведения атаки типа отказ в обслуживании.

Примечание. Сотрудники OSINT должны проконсультироваться с помощником начальника штаба по вопросам связи/офицером связи (S-6/G-6) и сотрудниками отдела обеспечения информационной безопасности для ознакомления с существующими компьютерными угрозами и руководящими принципами, а также проверки операционных систем и браузеров, что в настоящее время используются новейшие антивирусные программы и контрразведывательное программное обеспечение.

ПРИЛОЖЕНИЕ D

ПОЛЬЗА РАЗВЕДКИ В ОТКРЫТЫХ ИСТОЧНИКАХ (OSINT)

Содержание данного приложения указывает на то, как интеграция разведки в открытых источниках (OSINT) поддерживает и способствует:

- Объединенным наземным операциям, связанным с ними миссиям и задачам;

- Другим дисциплинам разведки;
- Другим функциям, в частности, работе с вебсайтами (SE), проверке и анализу источника.

Приведенные примеры представляют собой неполный список.

Поддержка процесса анализа цели (противника), борьбы с повстанцами и самодельными взрывными устройствами

D-1. Информация из открытых источников используется при составлении списка целей (сил противника) и справочной информации, подготовке брифинга и требований командования. Следующий пример описывает одну ситуацию, когда разведка в открытых источниках способствует сбору данных о цели. (Более подробную информацию см. в FM 3-60).

Пример 1: Разведка в открытых источниках способствует подготовке операции

Соединенные Штаты Америки (США) вступают в войну против государства X. Основной целью США является снижение возможностей государства X для ответного удара. У государства X имеется хранилище значительного военного запаса вооружения, который намеренно расположен вблизи религиозного центра. Следует ли США нанести ракетный удар по данному хранилищу, осознавая, что есть большая вероятность уничтожения религиозного центра? Сотрудники OSINT могут поддерживать данную операцию путем предоставления ответов на следующие вопросы:

- Какова религиозная принадлежность населения, проживающего рядом с религиозным центром?
- Имеет ли религиозный центр культурное значение?
- Является ли данный центр историческим достоянием?
- Какая часть населения посещает данный центр?
- В какое время большинство людей посещают данный центр?
- Какие тактико-технические характеристики вооружения в хранилище?

D-2. При поддержке операций против повстанцев, информация из открытых источников является важным аспектом для понимания оперативной обстановки, выявления общественного мнения и поддержки, оказываемой

повстанцам. Общедоступная информация также является важным средством для определения эффективности информирования и воздействия среди местного населения. Мониторинг СМИ также оказывает поддержку подобным операциям.

В соответствии с приоритетными требованиями разведки (PIRs), мониторинг должен осуществляться на каждом уровне разведывательного органа. Крупные новостные сети постоянно анализируются и подлежат проверке на уровне корпуса (соединения), однако на тактико-оперативном уровне, в первую очередь, анализу и проверке должны подлежать местные газеты и радиостанции. (Для получения дополнительной информации об операциях против повстанцев, см. FM 3-24).

Поддержка других методов разведки

D-5. Обработанная и проанализированная информация из открытых источников может также использоваться в поддержку других методов ведения разведки.

Агентурная разведка

D-6. Разведка в открытых источниках (OSINT) поддерживает агентурные операции с помощью предоставления обработанных материалов из открытых источников начальнику или офицеру штаба агентурной разведки и контрразведки, а также ведомствам разведывательного сообщества и связующим подразделениям. Ниже указан неполный список подобных материалов:

- Карты;
- Чертежи;
- Каталоги телефонов;
- Бизнес-каталоги;
- Газеты;
- Видео- и аудио материалы (Пример: кассеты и компакт-диски).

D-7. Для получения дополнительной информации об агентурных операциях по сбору информации, см. FM 2-22.3.

Радиоэлектронная и геопространственная разведка

D-8. Разведка в открытых источниках (OSINT) непосредственно используется в поддержку радиоэлектронной (РЭР-SIGINT) и геопространственной разведок (GEOINT).

Пример 2: Использование разведки в открытых источниках для поддержки РЭР

- Офицер связи подразделения С готовит план предстоящей операции. Данный офицер не имеет доступа к секретным системам связи. Подразделение С готовится к проведению операции в районе, где средства массовой информации контролируются тоталитарным режимом. Использование разведки в открытых источниках (OSINT) может предоставить следующую информацию:

- Выявление местных телевизионных каналов, их вспомогательных компонентов и систем;
- Вебсайты, используемые для воздействия на местное население.

Пример 3: Использование разведки в открытых источниках для поддержки геопространственной разведки

Во время планирования миссии, инженер D выявляет возможные последствия строительства новой железнодорожной системы. Данная железнодорожная система разделит сельскохозяйственное сообщество, вдоль основного пути орошения. Существует потенциальная угроза, что железнодорожная система нарушит и повредит оросительные каналы. Для запроса, спутниковых снимков, обеспечивающих наглядную панораму области, существуют временные ограничения. Если железнодорожная система повредит оросительные каналы, то это негативно скажется на отношениях между руководством подразделения и племенными вождями. Разведка в открытых источниках (OSINT) также может поддерживать визуальную разведку (фоторазведка-IMINT) путем предоставления снимков из «Google Earth» и других коммерческих фотографий для определения альтернативных русел рек, будущих районов слива после орошения, а также потенциальных районов затопления в случае наводнения.

Техническая разведка и контрразведка

D-9. Использование общедоступной информации является важным аспектом технической разведки (TECHINT). Несмотря на то, что намерения, возможности и факторы уязвимости противников и потенциальных угроз подлежат засекречиванию, результаты технологического прогресса в виде сети Интернет и программы «Google Earth» способствуют получению

информации о самых скрытных государствах и организациях. (Для получения дополнительной информации о TECHINT см. TC 2-22.4.)

D-10. При поддержке контрразведывательных (CI) операций, общедоступная информация может быть использована для получения данных, которые соответствуют приоритетным требованиям разведки (PIRs) и другим постоянным требованиям контрразведки (CI). Разведкой в открытых источниках (OSINT) Сухопутных войск США занимаются бригады военной разведки. Военнослужащие («Солдаты») военной разведки получают курсы подготовки к ведению разведки в открытых источниках (OSINT) в специальных школах обучения. По прибытии в места прохождения службы и в соответствии с задачами разведывательного подразделения, военнослужащие должны пройти подготовку по ведению разведки в открытых источниках (OSINT). (Для получения дополнительной информации о контрразведке (CI), см. FM 2-22.2.)

ПРИЛОЖЕНИЕ Е

ОРГАНИЗАЦИИ, ЗАНИМАЮЩИЕСЯ РАЗВЕДКОЙ В ОТКРЫТЫХ ИСТОЧНИКАХ

Ведение разведки в открытых источниках повышает эффективность деятельности всего разведывательного сообщества США, начиная национальным и заканчивая тактическим уровнями. Некоторые государственные органы, такие как министерство обороны, правоохранительные органы, и другие ведомства, занимающиеся сбором, приобретением, использованием, анализом, распространением информации из открытых источников:

- Совет по защите открытых источников (DOSCI);
- Командование разведки и безопасности ВС США (INSCOM);
- Служба разведывательной информации Департамента сухопутных войск (DA IIS).
- Директор национальной разведки центра открытых источников (DNI OSC).
- Академия открытых источников;
- Департамент передовых систем (ASD).
- ФБР.
- Федеральный научно-исследовательский отдел (FRD), библиотека Конгресса.

Совет по защите открытых источников (DOSCI)

Е-1. Совет по защите открытых источников является основным правовым механизмом ведения разведки в открытых источниках министерства обороны США. Она служит форумом для координации и содействия мероприятиям и программам ведения разведки в открытых источниках для всех служб и боевых команд. Данный совет консультирует и докладывает заместителю министра обороны по разведке о вопросах ведения разведки в открытых источниках, о новых инициативах по улучшению эффективности работы подразделения OSINT и деятельности министерства обороны в целом. В

обязанности совета входят:

- координирует деятельность подразделения OSINT и утверждает его план ведения разведки в открытых источниках;
- определяет последовательность требований к процессу ведения разведки в открытых источниках.

Командование разведки и безопасности ВС США (INSCOM)

Е-2. Командование разведки и безопасности ВС США проводит разведывательных операций в открытых источниках для сбора, анализа, подготовки разведывательных материалов и его дальнейшего использования; управляет базой данных разведывательной системы СВ США, а также обеспечивает специализированными возможностями быстрого реагирования, повышение квалификации и лингвистическая поддержка при развертывании сил, с целью оказания поддержки объединенным наземным операциям.

Е-3. INSCOM регионально поддерживает каждое из объединенных командований ВС США с помощью подчиненных ему региональных многофункциональных бригад военной разведки.

Каждая бригада определяет разведывательные требования (включая ведение разведки в открытых источниках) и обеспечивает поддержку развертывания тактических подразделений Сухопутных войск или оперируют в составе объединенных командований в зонах ответственности и регионе проведения военной операции. Каждая многофункциональная бригада имеет возможность вести разведку в открытых источниках, направлять запросы в вышестоящие разведывательные ведомства и отвечать запросам подчиненных подразделений на тактическом уровне с помощью программы OSCAR-MS.

Служба разведывательной информации Департамента Сухопутных войск (DA IIS)

Е-4. Данная служба оказывает широкий спектр разведывательной поддержки Сухопутным войскам и всему разведывательному сообществу, а также управлению требованиями к процессу сбора информации из открытых источников.

Она находится в подчинении помощника начальника штаба по разведке, отделения по управлению разведывательной информацией (DAMI-IM), а

оперативный контроль осуществляется помощником начальника штаба по боевым операциям командования разведки и безопасности ВС США. Данная служба является основным органом распределения разведывательной информации в Сухопутных войсках.

Е-5. Основной миссией службы разведывательной информации департамента Сухопутных войск является координация, распространение и проверка стратегических запросов по требованиям к открытым источникам в масштабе СВ под руководством помощника начальника штаба по разведке. Это осуществляется путем предоставления и обмена информацией между разведывательными ведомствами.

Данная служба входит в состав подкомитета управления требованиями сбора информации Национального центра открытых источников при Управлении директора национальной разведки (ODNI).

Служба охватывает все аспекты ведения разведки в открытых источниках: концепцию, подготовку кадров, оперативную поддержку, сбор, обработку, анализ и распространение информации.

Директор национальной разведки Центра открытых источников

Е-6. Директор центра открытых источников национальной разведки по указанию помощника заместителя директора национальной разведки в открытых источниках (ADDNI / OS) поддерживает деятельность Национального комитета открытых источников. Центр открытых источников (ЦОИ) входит в состав разведывательного сообщества, правительства США, частного сектора и научных кругов.

Е-7. В своей деятельности ЦИО руководствуется положением требований к открытым источникам, которые находятся в утвержденном ежегодном плане ЦИО по сбору информации в открытых источниках. Данный центр имеет всемирную сеть многоязычных региональных экспертов, которые подготавливают ответы на информационно-разведывательные требования, используя общедоступную информацию из открытых источников, таких как радио, телевидение, газеты, информационные агентства, базы данных и Интернет.

Центр открытых источников осуществляет мониторинг открытых источников в более чем 160 странах на 80 языках и проводит сбор общедоступных информации по всему миру. Собранный материал центр направляет в министерство обороны, правительственные учреждения, а также местные отделы правоохранительных органов США.

Е-8. Службы и инструменты ЦОИ оказывают содействие агентствам и отделениям правительства и разведывательного сообщества США при проведении разведки в открытых источниках, создавая условия для создания, управления и распространения несекретной информации.

Эффективность и адаптивность инструментов Центра открытых источников:

- Продвинуто для использования открытых источников и создания разведывательных справок;
- Предназначен для обеспечения поддержки и предоставления ресурсов для децентрализованной клиентской базы через Интернет. Является легко доступным.

- Соответствует стандартам безопасности, технического развития и метаданных разведывательного сообщества;

Е-9. Центр открытых источников анализирует содержание и поведение иностранных СМИ и интернет-сайтов и других международных организаций, представляющих значительный интерес политике правительства США.

Академия открытых источников

Е-10. Академия открытых источников предоставляет обучение методике конспирации в открытых источниках. В связи с увеличением степени использования разведанных из открытых источников (см. таблицу Е-1), все больше сотрудников государственных учреждений проходят курсы подготовки при Академии открытых источников, с целью получения навыков и освоения, изменяющихся OSINT технологий. Академия открытых источников строит отношения с руководителями всех разведывательных организаций для разработки комплексного подхода к обучению навыков конспирации при ведении разведки в открытых источниках. В академии проходят курс обучения сотрудники Министерства обороны, федеральных агентств, а также местных органов правопорядка.

Таблица Е-1. Преподаваемые предметы в Академии открытых источников

<ul style="list-style-type: none">• Введение;• Библиотечные ресурсы и методы исследования;	<ul style="list-style-type: none">• Методология визуального убеждения: Расширенный поиск в Google;
---	--

<ul style="list-style-type: none"> • Анализ СМИ; • Рабочий среда нового пользователя; • Исследования и анализ открытых источников; • Ознакомление с Центром открытых источников; • OS 101: Основы открытых источников; • OS 201: Открытые источники 201; <ul style="list-style-type: none"> • Разведка в открытых источниках (OSINT) и другие разведки; • Обзор требований к процессу сбора информации Центра открытых источник; • Угрозы безопасности и конфиденциальности для интернет-пользователей; • «Умный поиск» - Использование ресурсов библиотеки; • Интенсивные курсы ведения OSINT; • Инструменты и источники данных. 	<ul style="list-style-type: none"> • Методология по выявлению общественного мнения; • Семинар по классификации открытых источников; • Системы цифровые аудио- и видео-средств (DAVE); • Создание мультимедийных устройств; • Обзор Цифровые аудио- и видео-средств (DAVE); • Краткий обзор цифрового аудио- и видеооборудования; • Распределение информации; • Основы анализа открытых источников; • Управление над тактическим полем; • Основы Центра открытых источников подготовки и операций с текстом (PROPS); • Введение в анализ геопространства; • Тайные вселенные информации в Интернете; • Высокопроизводительная рабочая станция «Block II 101»; • Высокопроизводительная рабочая станция «Block II 201».
--	---

Подразделение Сухопутных войск США по изучению азиатского региона

Е-11. Подразделение Сухопутных войск США по изучению азиатского региона (ASD) является старейшим и крупнейшим, а также одним из самых прочно обоснованных подразделения министерства обороны по ведению

разведки в открытых источниках (OSINT). Данное подразделение демонстрирует характеристики устоявшегося механизма по эксплуатации методов OSINT. В частности, ASD занимается сбором, анализом, обработкой, использованием открытых данных, а также подготовкой кратко- и среднесрочных отчет-анализов общедоступной информации о военном потенциале, угрозах безопасности войск и других разведанных оперативного характера о странах, войсках и негосударственных организациях, действующих в зоне ответственности Объединенного Тихоокеанского командования ВС США. Подобные требования включают в себя возможности, расположение и готовность Вооруженных сил НОАК, КНДР и Дальнего Востока РФ, а также оборонную тематику, связанную с Южной и Юго-Восточной Азией. В состав рабочего персонала подразделения входят гражданские сотрудники министерства и резерва Сухопутных войск, а также военнослужащие Национальной гвардии, которые занимаются руководством и подготовкой миссий подразделения.

Также в ASD работают иностранные сотрудники, финансируемые правительством Японии, для осуществления сбора, анализа, перевода, подготовки справок-докладов и ведения баз данных.

Е-12. Основная задача ASD заключается в сборе, анализе, использовании и подготовке докладов о данных из иностранных открытых источников, в соответствии с информационно-разведывательными требованиями Объединенного Тихоокеанского командования ВС США (USPACOM) и командования СВ США в зоне Тихого океана, а также других национальных интересов. При ведении разведки в открытых источниках, специалисты подразделения ASD используют печатные и Интернет-материалы из СМИ.

Е-13. Сотрудники ASD добывают информацию для подготовки соответствующего аналитического материала с помощью программы OSCAR-MS. ASD указывает ссылки на открытые источники в формате разведывательного доклада, схожего с научными статьями или исследованиями. Текущий раздел операций ASD предоставляет ежедневную сводку, содержащую статьи из прессы, отражающих мнение иностранного сообщества о политике и интересах США. Услуги и инструменты, которые предоставляет ASD:

- Разведанные из открытых источников, соответствующие требованиям

сети «OSCAR-MS»;

- Аналитические доклады разведки в открытых источниках.;
- Ежедневные доклады о защите войск/ситуационной осведомленности (FPSARs);
- Ежедневный доклад разведки в открытых источниках об положении и окрестностях Японии (ASJORs);
- Ежедневная ситуационная сводка (SITREPs);
- Еженедельная репортажи военных фотографий о Китае и Тайване;
- Специальная отчетность по запросу пользователей OSCAR-MS;
- Распределение разведанных из открытых источников в незащищенной (NIPRNET) и защищенной (SIPRNET) сетей интернет-маршрутизаторов, а также объединенной коммуникационной системы предупреждения об угрозах (JWICS);
- Карта сбора информации;
- Доклады по информации из СМИ.

Федеральное бюро расследований

E-14.ФБР является ведомством при Министерстве юстиции, которое служит в качестве федерального следственного органа и подразделения внутренней разведки. ФБР подследственную юрисдикцию над нарушениями более чем 200 категорий федеральных преступлений.

E-15. Основными задачами ФБР являются предотвращение и защита США от террористических и внешних угроз со стороны иностранных спецслужб, а также поддержание уголовного законодательства государства. Это достигается с помощью постоянного контроля конкретных категорий, которые включают, но не ограничиваются:

- ограбление банка;
- ограбление и вымогательство, влияющие на межштатную торговлю;
- Распространение наркотиков;
- Заговор;
- Сексуальные связи с несовершеннолетними;
- Мошенничество с использованием почты;
- Мошенничество с банковскими операциями;
- Мошенничество через проводную и радиосвязь или телевидение;
- Незаконный бизнес, связанный с азартными играми.

Е-16.ФБР использует общедоступную информацию из открытых источников в области борьбы с терроризмом, контрразведки (СІ), киберпреступности, информационных технологий и судебной практики. Услуги и инструменты ФБР включают, но не ограничиваются:

- Сводка правоохранительных органов;
- Составление карты-преступности;
- Статистика (киберпреступность, должностные и насильственные преступления).

Федеральный научно-исследовательский отдел при библиотеке Конгресса США

Е-17. Федеральный научно-исследовательский отдел при библиотеке Конгресса США (FRD) был создан во время Второй мировой войны для сбора и проведения исследований, захваченных авиационных и технических докладов о немецких и японских войсках. Данный материал позволял лучше понимать будущий курс оборонительного развития страны, а также поддерживать разведывательных усилия, приведших к победе над державами «оси», странами нацистского блока.

Е-18.Миссия FRD заключается в обеспечении направленного исследования и анализа внутренних и международных субъектов, работающих в ведомствах правительства США, округе Колумбия, а также уполномоченных федеральных подрядчиков. Данный отдел осуществляет научно-исследовательскую деятельность в открытых источниках под руководством библиотеки Конгресса США. FRD предоставляет следующие услуги и инструменты:

- Оригиналы исследовательских материалов, включая доставку документов;
- Абстрагирование и перевод иностранных языков;
- Аннотированные библиографии;
- Организационные и законодательные данные;
- Исследования и доклады;
- Книги;
- Военные нормативно-правовые ресурсы;
- Исследования стран мира;
- Справки о странах мира;
- Терроризм, уголовные исследования и оценки.

ПРИЛОЖЕНИЕ F

РЕСУРСЫ ОТКРЫТЫХ ИСТОЧНИКОВ

При проведении исследования, сотрудники разведки имеют доступ к широким объемам информации. Понимание и осознание того, где нужно начинать поиск конкретной информации является важным фактором для эффективности работы аналитика. В нижеуказанных таблицах указаны некоторые первоначальные пункты для получения информации, которая может быть обработана и подготовлена в виде разведывательных данных.

Таблица F-1 содержит военные открытые источники.

РАЗВЕДЫВАТЕЛЬНАЯ СЕТЬ ОБМЕНА ДАННЫМИ (IKN)
<p>IKN - это инструмент управления данными, который позволяет сотрудникам («Солдатам») по всему миру общаться, сотрудничать и проводить расследования. В IKN входит:</p> <ul style="list-style-type: none">• Проведение дискуссионных форумов;• Сеть служит в качестве единой точки входа в Центр повышения квалификации военной разведки США (USAICoE) и другие сайты разведывательного сообщества;• Поддерживает различные общественные и частные веб-приложения, которые помогают разведывательному сообществу.
УНИВЕРСИТЕТ ВОЕННОЙ РАЗВЕДКИ (UMI)
<p>UMI является подразделением дистанционного обучения школы военной разведки. С веб-сайта UMI, профессионалы военной разведки могут получить доступ к:</p> <ul style="list-style-type: none">• Самостоятельному и дистанционному обучению;• Центру интеграции иностранных языков и культуры;• Учебным ресурсам военной разведки.
РАЗВЕДЫВАТЕЛЬНАЯ ОНЛАЙН БАЗА ДАННЫХ СУХОПУТНЫХ ВОЙСК (АКО)
<p>Разведывательная онлайн база данных сухопутных войск (АКО) включает:</p> <ul style="list-style-type: none">• Центр обмена разведывательной информации;• Центр знаний (документы, боевой устав (FMs); техническая связь (ТС); тактику, методы и процедуры СВ США (ATTPs); и др.);• Обучение, учреждения, политику, доктрины, а также ссылки на другие веб-сайты, связанные с разведкой.
ПРОГРАММА ОТКРЫТЫХ ИСТОЧНИКОВ «АКО»
<p>Программа открытых источников «АКО» предлагает общедоступные:</p> <ul style="list-style-type: none">• События;• Разведданные;• Дискуссионные форумы;• Справочники;• Интересуемые ссылки.

<p>БИБЛИОТЕКА ВОЕННОЙ РАЗВЕДКИ: Доступна с помощью домашних страниц IKN и форума «Warfighter»</p>
<p>Центр отчетности при библиотеке военной разведки содержит множество баз данных и ресурсов:</p> <ul style="list-style-type: none"> • Журналы и газеты; • Исторические документы; • Формы и публикаций; • Чтения в области культуры; • Руководство доступных источников; • Учебный центр военной разведки по изучению иностранных языков (MIFLTC)
<p>ИССЛЕДОВАТЕЛЬСКИЙ ПОРТАЛ СЛУЖБА РАЗВЕДЫВАТЕЛЬНОЙ ИНФОРМАЦИИ МИНИСТЕРСТВА СВ (DA IIS): Данный портал доступен на домашней странице АКО</p>
<p>Данный портал создан на основе структурных, схематичных и систематизированных сетей, удобных для оперативного и быстрого поиска разведывательной информации. Ниже указаны некоторые ссылки из данного вебсайта:</p> <ul style="list-style-type: none"> • Документы из открытых источников – программы «Early Bird», ежедневное обновление на тему «Терроризм», Интернет вестники «Baghdad Mosquito», «Basra Bugle» и другие; • Разведывательное сообщество; • Боевые командования; • Ссылки аналитиков; • Поисковые программы. <p><i>Примечание.</i> С целью предоставления всей необходимой информации для успешного выполнения операции, доступ к данным осуществляется через несколько сетей.</p>
<p>ВНУТРЕННЯЯ РАЗВЕДЫВАТЕЛЬНАЯ СЕТЬ «INTELINK-U»</p>
<p>Intelink-U является сетью внутренней связи Департамента национальной разведки (DNI) для сотрудничества с другими государственными учреждениями (ведомствами). Intelink-U:</p> <ul style="list-style-type: none"> • Находится под руководством управления «Intelink Management Office»; • Предоставляет совместное использование, удаленный доступ и услуги

<p>доступа и обработки несекретной оперативной и общедоступной информации;</p> <ul style="list-style-type: none"> • Обеспечивает защищенную среду для обмена несекретной; чувствительной, но несекретной информации и информации для служебного пользования среди сотрудников министерства обороны. <p><i>Примечание. Доступ к услугам сети Intelink-U осуществляется через несколько виртуальных частных сетей.</i></p>
<p>ОБЪЕДИНЕННЫЙ УЧЕБНЫЙ ЦЕНТР ВОЕННОЙ РАЗВЕДКИ:</p>
<p>Армий мира</p>
<ul style="list-style-type: none"> • Вооруженные силы мира <p><i>Примечание. Для доступа к странице требуется пользовательская регистрация учетной записи.</i></p> <ul style="list-style-type: none"> • Общевоинская научно-исследовательская библиотека
<p>ЦЕНТР ИЗУЧЕНИЯ ОПЫТА ДЕЙСТВИЙ ЧАСТЕЙ И СОЕДИНЕНИЙ СВ (CALL)</p>
<ul style="list-style-type: none"> • CALL
<p>БОЕВЫЕ ОПЕРАЦИИ В ГОРОДСКИХ УСЛОВИЯХ (MOUT)</p>
<ul style="list-style-type: none"> • MOUT
<p>СЛУЖБЫ ВОЕННОЙ РАЗВЕДКИ</p>
<ul style="list-style-type: none"> • Командование разведки и безопасности СВ США (INSCOM); • Управление военно-морской разведки; • Агентство разведки, наблюдения и рекогносцировки (ISR) ВВС США; • Разведывательная деятельность Корпуса морской пехоты США
<p>РАЗВЕДЫВАТЕЛЬНЫЕ СЛУЖБЫ ОБЪЕДИНЕННЫХ КОМАНДОВАНИЙ ВС США</p>
<ul style="list-style-type: none"> • Объединенное центральное командование ВС США; • Объединенное командование ВС США в Европе; • Объединенное тихоокеанское командование ВС США; • Объединенное командование ВС США в зоне Центральной и Южной Америки; • Объединенное командование ВС США в зоне Африки; • Объединенное командование военно-космических сил ВВС США; • Объединенное командование специальных операций ВС США; • Объединенное стратегическое командование ВС США;

•Объединённое командование стратегических перебросок ВС США (TRANSCOM).

Информация Исследовательского Центра Виктора Воксанаева

Книги Воксанаева В.П.

1. Книга: «Контрразведка по открытым источникам»



Издательство 2010 г.

ISBN 978-5-98864-033-2

твёрдый переплет, объем 352 стр., тираж – 100 экз.

книга распространяется на возмездной основе. Заявка на [voksanaev\[at\]mail\[dot\]ru](mailto:voksanaev[at]mail[dot]ru)

Для ВУЗов и библиотек России книга распространяется бесплатно (желающим обращаться по электронной почте, указанной на сайте Центра)

2. Книга: «Разведка по открытым источникам: уроки прошлого»

Автор: В. П. Воксанаев

Издательство: «Поверенный», 2007 г.

ISBN 5-93550-188-5

Мягкий переплет, объем 174 стр., тираж - 100 экз.

Публикация распространяется на возмездной основе.

Заявка на заказ - обращаться по электронной почте, указанной на сайте Центра.

Для ВУЗов и библиотек России публикация распространяется бесплатно (желающим обращаться по электронной почте, указанной на сайте Центра)

Виктор Воксанаев

Разведка по открытым источникам: уроки прошлого

**Разведка по открытым источникам:
уроки прошлого**

