Содержание

От издательства **7**
Предисловие к восьмому изданию **8**
Список сокращений **9**
Тезаурус **13**
Введение. Ситуация в России глазами экономиста в штатском **30**
Глава 1. Основы теории разведывательной информации **53**
1.1. Введение 53
1.2. Характеристики и требования к разведывательной информации 54
1.2.1. Качественные характеристики 55
1.2.2. Количественные характеристики 57
1.2.3. Ценностные характеристики 58
1.3. Источники и методы получения информации 67
1.3.1. Открытые источники информации 67
1.3.2. Косвенные (демаскирующие) разведывательные признаки 69
1.3.3. Оперативная информация 73
1.3.4. Экспертная информация 76
1.3.5. Агентурная информация 78
1.3.6. Использование возможностей сторонних организаций 78
1.4. Нормативно-правовые акты, регулирующие оборот информации в РФ 80
Глава 2. Система экономической разведки промышленного предприятия **85**
2.1. Введение 85
2.2. Цели создания системы экономической разведки предприятия 86
2.3. Потребности в разведывательной информации на предприятии 87
2.4. Организационные принципы системы экономической разведки предприятия 88
2.5. Принципы финансирования системы экономической разведки предприятия 90
2.6. Обеспечение собственной безопасности системы экономической разведки 94
2.7. Вывод 98
Приложение 1. Форма заявки-задания на проверку 98
Глава 3. Система экономической контрразведки промышленного предприятия **102**
3.1. Введение 102
3.2. Обоснование необходимости создания контрразведывательного подразделения в структуре службы безопасности предприятия 103
3.3. Планирование контрразведывательной деятельности 105

3.4. Несколько практических советов по методологии организации работы подразделения экономической контрразведки ... 106
3.5. Практика применения DLP-систем в работе подразделения экономической контрразведки ... 113
3.6. Теория и практика оперативных игр в работе подразделения экономической контрразведки ... 116

Глава 4. Информационно-поисковая работа: привлечение к доверительному сотрудничеству ... 120

4.1. Введение. Краткая историческая справка ... 120
4.2. Классификация информаторов ... 126
4.2.1. Классификация информаторов по их назначению ... 127
4.2.2. Классификация информаторов по степени доверия ... 129
4.3. Этапы вербовочной разработки и их содержание ... 130
4.3.1. Выявление кандидатов ... 131
4.3.2. Оценка способностей и мотивации ... 132
4.3.3. Первичный контакт ... 136
4.3.4. Период установления доверия. Создание расположения к себе ... 140
4.3.5. Привлечение к сотрудничеству объекта вербовочной разработки ... 143
4.3.6. Закрепление оперативного контакта ... 152
4.3.7. Проверка доверительного помощника ... 154
4.3.8. Обучение доверительного помощника ... 157
4.3.9. Руководство деятельностью доверительного помощника ... 161
4.3.10. Завершение контакта ... 174
Приложение 1. Агенты влияния ... 175

Глава 5. Информационно-поисковая работа: использование возможностей сторонних организаций ... 183

5.1. Российские министерства, ведомства и государственные аналитические центры ... 183
5.1.1. Федеральная налоговая служба РФ ... 183
5.1.2. Банк России ... 184
5.1.3. Федеральная служба государственной статистики РФ ... 184
5.1.4. Портал государственных закупок РФ ... 185
5.1.5. Государственная автоматизированная система РФ «Правосудие» ... 185
5.1.6. Генеральная прокуратура РФ ... 186
5.1.7. Министерство внутренних дел РФ ... 187
5.1.8. Министерство юстиции РФ ... 187
5.1.9. Федеральная антимонопольная служба РФ ... 188
5.1.10. Федресурс ... 188
5.1.11. Федеральная нотариальная палата РФ ... 189
5.1.12. Федеральная служба по интеллектуальной собственности РФ ... 189
5.1.13. Федеральное архивное агентство РФ ... 190
5.1.14. Федеральная служба по надзору в сфере образования и науки РФ ... 191
5.1.15. Министерство иностранных дел РФ ... 191
5.1.16. Государственные аналитические центры РФ ... 191

5.2. Российские частные информационные агентства ... 193
5.2.1. Группа компаний «Интегрум» ... 193
5.2.2. ООО «Коммерсантъ КАРТОТЕКА» ... 193
5.2.3. Группа «Интерфакс» ... 194
5.2.4. Группа компаний «Кронос-информ» ... 194
5.2.5. ООО «Система комплексного раскрытия информации и новостей» (ООО «СКРИН») ... 195
5.2.6. Группа компаний «СКБ Контур» ... 195
5.2.7. Региональные информационные агентства ... 196
5.2.8. ООО «Центр анализа стратегий и технологий "АСТ-Центр"» ... 196
5.2.9. Проект «Школа молодого этнополитолога» ... 197
5.3. Бюро кредитных историй ... 198
5.3.1. Иностранные кредитные бюро ... 198
5.3.2. Российские кредитные бюро ... 208

Глава 6. Информационно-аналитическая работа: основные принципы ... 214

6.1. Введение ... 214
6.2. Информационная система службы безопасности предприятия ... 220
6.3. Базы данных «серого» и «черного» информационных рынков ... 232

Глава 7. Информационно-аналитическая работа: создание информационной системы службы безопасности предприятия ... 233

7.1. Введение ... 233
7.2. Краткая историческая справка ... 234
7.3. Модели представления данных в электронных базах данных ... 235
7.4. Программное обеспечение, используемое для создания информационной системы службы безопасности предприятия ... 246
7.5. Преимущества и риски использования систем искусственного интеллекта ... 252

Глава 8. Информационно-аналитическая работа с открытыми источниками информации ... 303

8.1. Роль и место открытых источников информации в работе разведывательных органов ... 303
8.1.1. Введение в специальность ... 303
8.1.2. Этапы развития технологий разведывательного анализа открытых источников ... 310
8.1.3. Исторический обзор практического использования технологий сбора и обработки материалов открытого доступа ... 316
8.1.4. Происхождение и содержание термина OSINT (Open Source INTelligence) ... 341
8.2. Методология работы с открытыми источниками информации ... 365
8.2.1. Использование сторонних возможностей по обработке СМИ ... 366
8.2.2. Использование собственных возможностей по обработке открытых источников информации ... 367
8.2.3. Аналитическая обработка ... 386
Приложение 1. Пример решения глобальной информационно-аналитической задачи ... 393
Приложение 2. Пример подготовки информационного документа ... 409

Приложение 3. Пример журналистского расследования на основании комплексного исследования ряда открытых источников информации 412

Глава 9. Аналитическая разведка средствами телекоммуникационной сети Интернет 417

9.1. Введение. Краткая историческая справка 417

9.2. Роль и место аналитической разведки средствами телекоммуникационной сети Интернет 422

9.3. Поиск в сети Интернет 429

9.3.1. Указание адреса страницы 430

9.3.2. Поиск по каталогам и передвижение по гиперссылкам 431

9.3.3. Поисковые системы 432

9.3.4. Обращение к специализированным сервисам 441

Приложение 1. Небольшой практикум 475

Приложение 2. Пример подготовки информационного документа 476

Глава 10. «Активные мероприятия»: информационно-психологическое воздействие 478

10.1. Введение. Краткая историческая справка 478

10.2. Основная часть. Теория и практика проведения активных мероприятий 480

10.2.1. Методы проведения активных мероприятий 481

10.2.2. Формы проведения активных мероприятий 487

10.2.3. Силы и средства проведения активных мероприятий 487

10.2.4. Планирование активных мероприятий 490

10.2.5. Проведение активных мероприятий средствами СМИ и СМК 496

Приложение 1. Открытое письмо директору АБВГДейки генералу армии Б. Лаврентию от заслуженных деятелей отечественной поп-культуры в связи с рейдерским захватом собственности доктора кукольных наук Карабаса Барабаса 510

Глава 11. Информационно-аналитическая работа: дезинформация 513

11.1. Введение. Краткая историческая справка 513

11.2. Теория и практика дезинформационных мероприятий 523

Глава 12. Кадровая работа: профессиональный портрет рыцаря плаща и гроссбуха 538

Глава 13. Экономическая разведка и контрразведка в истории развития цивилизации 560

13.1. Истоки промышленного шпионажа 560

13.2. Экономическая разведка и контрразведка в современном обществе 566

13.3. Заключение 598

Библиография 599

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте *www.dmkpress.com*, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу *dmkpress@gmail.com*; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу *http://dmkpress.com/authors/publish_book/* или напишите в издательство по адресу *dmkpress@gmail.com*.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу *dmkpress@gmail.com*. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты *dmkpress@gmail.com*.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Предисловие к восьмому изданию

Дорогие друзья!

С далеких времен людей интересовало, можно ли предугадать будущее. Утвердительно на этот вопрос отвечали только профессиональные астрологи, хироманты и… аналитики специальных служб.

Наступивший XXI век стал веком информационного общества, так как информация – это единственный на сегодня известный человеку ресурс, который со временем только увеличивается. Использование информационного ресурса открывает перед человеком новые возможности, о которых даже и не подозревали футурологи и фантасты.

Сегодня выжить и обеспечить себе успех в условиях наступившей глобализации смогут только те, кто максимально успешно приспосабливается к постоянно меняющимся условиям. Сделать это в короткие сроки и с наименьшими потерями помогает грамотно поставленная работа с информацией, о которой мы с вами по мере сил и возможностей продолжим разговор в новом издании этой книги.

В связи со сложной международной политической обстановкой нужно отметить, что часть иностранных правообладателей ограничили пользователям с российскими IP-адресами доступ к своим информационным ресурсам, поэтому, к сожалению, не все указанные в текущем издании ссылки на электронные источники могут работать должным образом.

Хочу высказать слова глубокой благодарности за помощь в работе над этой книгой В. А. Абрамову, В. В. Бабкину, К. Болгову, И. Н. Борисову, С. Г. Висичу, В. А. Воронину, Е. М. Губериной, О. Ю. Глухову, В. Е. Евсюкову, к. ю. н. Ю. К. Евтину, Б. П. Жмурко, к. т. н. доценту В. И. Иванкину, А. Н. Иванову, к. и. н. профессору Л. Г. Кедровской, А. Н. Кирилюку, к. т. н. доценту ТулГу С. А. Кузнецову, И. Л. Князеву, Н. К. Крылову, И. И. Ландеру, М. Ливенцовой, Б. И. Лобынцеву, С. В. Любимову, И. Н. Манжосу, президенту Консорциума «Инфорус» А. И. Масаловичу, Л. В. Митину, к. т. н. Е. А. Можарову, П. Мосенкову, А. Мыльникову, Н. В. Николотову, Н. М. Новичкову, С. В. Парфисенко, Н. Ю. Петрушову, М. Б. Пузакову, питерскому мегаэксперту с мировым именем в области безопасности Д. Ю. Пучкову (ст. о./у Гоблин), Е. Н. Путилову, С. И. Пучкову, С. А. Попову, А. Б. Соловьеву, Н. А. Тереб, Б. Е. Токареву, д. э. н. профессору Е. А. Федоровой, М. Финашиной, Н. И. Чадаеву, М. Е. Черкасову, Я. А. Чернину, к. т. н. С. И. Шатских.

Автор выражает благодарность за советы и консультации, полученные при написании этой книги от коллектива ГК «Кронос-Информ» и персонально от С. Г. Лобанова, Д. В. Платонова и Е. А. Бадовской; от информационно-аналитического агентства «Интегрум» в лице К. В. Кузнецова, В. В. Пешехонова, Е. Кузнецовой, А. Перепоновой и Д. Лисицына; а также от участников военно-исторического форума «ВИФ-2NE» (*www.vif2ne.org*) Н. Манвелова, В. Науменко, А. Никольского, Б. Седова, А. Солдатова, А. Словцова, а также от укрывшихся за никами У.Р.С.а, Оямы и 1071.

Отдельная благодарность коллективу издательства «ДМК Пресс», руководителю компании «Интернет-Розыск» Игорю Бедерову и автору проекта Russian OSINT.

Мой адрес для обсуждения нового издания книги: 3421@rambler.ru.

С уважением и надеждой на дальнейшее сотрудничество,
А. И. Доронин

Список сокращений

Общие сокращения

(См. также Тезаурус.)

АИС – автоматизированная информационная система.
АМ – активное мероприятие.
АО – акционерное общество.
БКИ – бюро кредитных историй.
БЧ – боевая часть.
ВВС – военно-воздушные силы.
ВМС – военно-морские силы.
ВМФ – военно-морской флот.
ГК – группа компаний.
ГПЭ – готовые поражающие элементы.
ГЭС – гидроэлектростанция.
ГРЭС – государственная районная электростанция.
ДМ – дезинформационное мероприятие.
ДИТ – Департамент информационных технологий.
ДП – доверительный помощник.
ЕИС – единая информационная система.
ЗАО – закрытое акционерное общество.
ЗРК – зенитный ракетный комплекс.
ИА – информационное агентство.
ИАС – информационно-аналитическая система.
ИИ – искусственный интеллект.
ИНН – идентификационный номер налогоплательщика.
ИПР – информационно-поисковая работа.
ИСУБД – инструментальная система управления базами данных.
ИТ – информационные технологии.
КК – конспиративная квартира.
КРП – конечный разведывательный продукт.
КЭС – конденсационная электростанция.
ЛПР – лицо, принимающее решение.
ЛЭП – линия электропередач.
МВД – министерство внутренних дел.
МИД – министерство иностранных дел.

МПК – международная патентная классификация.

МКТУ – международная классификация товаров и услуг.

МКПО – международная классификация промышленных образцов.

НДС – налог на добавленную стоимость.

НИИ – научно-исследовательский институт.

НИОКР – научно-исследовательские и опытно-конструкторские работы.

НИУ – национальный исследовательский университет.

НМПТ – наименования мест происхождения товаров.

НТЦ – научно-технический центр.

НЭП – новая экономическая политика; экономическая политика, проводившаяся с 1921 по 1928 годы в Советской России и СССР.

ОАО – открытое акционерное общество.

ОВР – объект вербовочной разработки.

ОГБ – органы государственной безопасности.

ООО – общество с ограниченной ответственностью.

ОПГ – организованная преступная группа.

ОПС – организованное преступное сообщество.

ОРД – оперативно-разыскная деятельность.

ОРМ – оперативно-разыскное мероприятие.

ОЭС – объединенная энергетическая система.

ПАО – публичное акционерное общество.

ПВО – противовоздушная оборона.

ПО – программное обеспечение.

ПРП – промежуточный разведывательный продукт.

РВСН – ракетные войска стратегического назначения.

РИ – разведывательная информация.

РП – разведывательный продукт.

РСФСР – Российская Советская Федеративная Социалистическая Республика.

РФ – Российская Федерация.

СБ – служба безопасности.

СВО – специальная военная операция.

СМИ – средства массовой информации.

СМК – средства массовой коммуникации.

СП – совместное предприятие.

СССР – Союз Советских Социалистических Республик (также известен как Советский Союз).

СУБД – система управления базами данных.

ТЭК – топливно-энергетический комплекс.

ТЭС – тепловая электростанция.

ТЭЦ – теплоэлектроцентраль.

ФГБУ – федеральное государственное бюджетное учреждение.

ФОИВ – федеральные органы исполнительной власти.

ФПГ – финансово-промышленная группа.

ЧВК – частная военная компания.

ЭЦП – электронная цифровая подпись.

AI (*англ.* Artificial Intelligence) – искусственный интеллект.

API (*англ.* Application Programming Interface) – программный интерфейс приложения.

BDA (*англ.* Battle Damage Assessment) – оценка боевого урона.

GAN (*англ.* Generative Adversarial Networks) – генеративно-состязательная сеть.

GL (*англ.* Grey, или Gray, Literature) – «серая» литература.

GR (*англ.* Government Relations) – выстраивание отношений с органами государственной власти.

IoT (*англ.* Internet of Things) – интернет вещей.

IT (*англ.* Information Technology) – информационные технологии.

KYC (*англ.* Know Your Customer – «знай своего клиента») – процедура верификации клиентов в компаниях.

LLM (*англ.* Large Language Model) – большая языковая модель (БЯМ).

LM (*англ.* Language Model) – языковая модель.

MA (*англ.* Managed Attribution) – управляемая атрибуция.

ML (*англ.* Machine Learning) – машинное обучение.

OSD (*англ.* Open-Source Data) – данные из открытых источников.

OSIF (*англ.* Open Source InFormation) – информация в открытом доступе.

PCR (*англ.* Public Credit Registries) – государственная регистрация кредитов.

PR (*англ.* Public Relations) – связи с общественностью.

SOCMINT (*англ.* Social Media Intelligence) – разведка в социальных сетях.

Организации

(См. также Тезаурус, страновые разделы.)

ВИНИТИ РАН – Всероссийский (во времена СССР – Всесоюзный) институт научной и технической информации РАН.

ВИМИ – Всероссийский (во времена СССР – Всесоюзный) научно-исследовательский институт межотраслевой информации.

ВСУ – Вооруженные силы Украины.

ВШЭ – Высшая школа экономики.

ИМВЭС НИУ ВШЭ – Институт мировой военной экономики стратегии факультета мировой экономики и мировой политики НИУ «Высшая школа экономики».

ЕПВ – Европейское патентное ведомство.

ЕЦБ – Европейский центральный банк.

ИНИОН РАН – Институт научной информации по общественным наукам РАН.

МАГАТЭ – Международное агентство по атомной энергии.

МГУ – Московский государственный университет.

РАН – Российская академия наук.

РИСИ – Российский институт стратегических исследований.

ТАСС – Телеграфное агентство Советского Союза, центральный информационный орган СССР.

ФАДН – Федеральное агентство по делам национальностей.

ФИПС – Федеральный институт промышленной собственности.

ШМЭП – Школа молодого этнополитолога.

API (*англ.* American Petroleum Institute) – Американский институт нефти.

BBCMS (*англ.* BBC Monitoring Service) – Служба прослушивания и перехватов.

CERN (Conseil Européen pour la Recherche Nucléaire) – Европейская организация по ядерным исследованиям.

EADS (*англ.* European Aeronautic Defence and Space Company) – авиационная и космическая компания.

IDC (*англ.* Interdepartmental Committee for the Acquisition of Foreign Publications) – Межведомственный комитет по приобретению иностранных публикаций.

FBIS (*англ.* Foreign Broadcast Intelligence Service) – Служба разведки иностранного вещания. Также известна как Foreign Broadcast Information Service – Информационная служба иностранного вещания, ранее FBMS (*англ.* Foreign Broadcast Monitoring Service) – Служба мониторинга иностранного вещания.

FDD (*англ.* Foundation for Defense of Democracies) – Фонд защиты демократий.

FBMS (*англ.* Foreign Broadcast Monitoring Service) – Службы мониторинга иностранного вещания.

NASDAQ (*англ.* National Association of Securities Dealers Automated Quotations) – американская биржа.

NTIS (*англ.* National Technical Information Service) – Национальная служба технической информации.

NYSE (*англ.* New York Stock Exchange) – Нью-Йоркская фондовая биржа.

PLC (*англ.* The Princeton Listening Center) – Принстонский центр мониторинга.

WSJ (*англ.* The Wall Street Journal) – американская деловая газета.

WNC (*англ.* World News Connection) – служба новостей на английском языке.

Тезаурус

Общая терминология

Агент влияния – 1) должностное лицо (либо лицо, пользующееся общественным доверием и авторитетом), осуществляющее систематическую деятельность по реализации целей политики иностранного государства (формально не являясь сотрудником его секретных служб); 2) общественный деятель, проводящий политику какой-либо партии или организации в среде, не принадлежащей к этим структурам; 3) к этой категории агентуры также можно отнести лиц, которые, хотя и не занимают видного общественного положения, могут оказывать информационно-психологическое влияние на объект воздействия. В этой роли могут выступать близкие родственники или друзья, любовник/любовница, священник и т. п.

Агентурные отношения – деловые отношения, складывающиеся между органами безопасности и их агентами в ходе использования агентов и решении конкретных контрразведывательных (разведывательных) задач. В агентурных отношениях участвуют две стороны: оперативные сотрудники как представители органов госбезопасности, и агенты как частные лица, давшие согласие (добровольно или вынужденно) оказывать на конспиративной основе помощь органам безопасности в решении стоящих перед ними задач.

Агентурные отношения регулируются системой правовых норм. Все основные, наиболее принципиальные стороны работы оперативного состава с агентами регулируются соответствующими приказами и инструкциями органов безопасности. Агентурные отношения начинают складываться с момента дачи вербуемым согласия секретно сотрудничать с органами безопасности. Заканчиваются агентурные отношения после прекращения связи с агентом.

Активные мероприятия (сокр. АМ, жарг. «активка») – специальные мероприятия, имеющие своей целью оказание выгодного влияния на политику органов исполнительной и законодательной власти для решения стоящих перед хозяйствующим субъектом задач; формирование благоприятного общественного мнения о нем, его руководстве и персонале; укрепление авторитета и доверия к нему среди партнеров и клиентов; стратегическое и тактическое дезинформирование конкурентов и оппонентов; подрыв и ослабление их позиций на рынке и в органах государственной власти.

В советских контрразведывательных органах под активными мероприятиями понимались «действия контрразведки, позволяющие ей проникнуть в замыслы противника, заблаговременно предупредить его нежелательные шаги, ввести противника в заблуждение, перехватить у него инициативу, сорвать его подрывные акции. Активные мероприятия в отличие от защитных мер, например по обеспечению режима секретности и сохранению государственной и военной тайны, носят наступательный характер и дают возможность вскрыть и пресечь враждебную деятельность на самой ранней стадии ее возникновения, заставить противника

обнаружить себя, навязать ему свою волю, вынудить его действовать в невыгодных условиях и в нужном органам контрразведки направлении. В практике контрразведывательной деятельности органов государственной безопасности к активным мероприятиям относят мероприятия по созданию агентурных позиций в лагере противника и его окружении, ведению оперативных игр с противником, по дезинформированию, компрометации и разложению сил противника, выводу на территорию СССР лиц, представляющих оперативный интерес, по добыванию разведывательной информации и т. д.»[1].

Аналитическая разведка – способ получения (в том числе и с помощью различных автоматизированных информационных систем и сервисов) новых сведений об объектах и явлениях, представляющих оперативный интерес, путем установления между ними причинно-следственных связей с целью подготовки дополнительных выводов и предложений о путях дальнейшего использования имеющейся информации об этих объектах и явлениях. Главным отличием аналитической разведки от методов информационно-поисковой работы является использование вторичных источников оперативных данных (отчетов, справок, докладов, публикаций и т. д.).

Атомарный факт (в контексте разведывательной деятельности) – минимальная единица информации, которая может быть использована для анализа и принятия решений. Такой факт не разлагается на составные элементы, состоит из одного элементарного суждения. На основе собранных атомарных фактов можно создать новый факт, то есть построить причинно-следственную цепочку.

Большие данные (*англ.* Big Data) – обозначение структурированных и неструктурированных данных огромных объемов и различных форматов, эффективно обрабатываемых с помощью специальных технологий. Термин Big Data появился в 2008 году в статье редактора журнала Nature Клиффорда Линча (Clifford Lynch), посвященной росту объемов информации. Автор статьи предложил термин по аналогии с выражениями «большая нефть», «большая руда».

Большая языковая модель (Large Language Model – LLM) – тип системы искусственного интеллекта, которая может распознавать и генерировать текст на любую тематику. LLM – высокопроизводительные программы, основанные на архитектуре трансформеров (transformer), способные «понимать» и генерировать текст с высокой степенью точности. Они совершенствуются с использованием методов машинного обучения, таких как «обучение с учителем» (*англ.* supervised learning), чтобы предсказывать следующее слово в последовательности или решать более сложные задачи, включая генерацию текста, машинный перевод и ответы на вопросы.

Вербовка – комплекс агентурно-оперативных мероприятий, направленных на выявление и привлечение к сотрудничеству лиц, способных дать или добыть полезную для спецслужб информацию.

---

[1] Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др.; М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.

Вербовочный контингент – часть социума, представители которой по оценке разведки обладают реальными или потенциальными возможностями участия в решении задач, стоящих перед разведывательным органом. Вербовочный контингент определяется под конкретную задачу и не является некой постоянной социальной структурой.

Вербовочная уязвимость – предрасположенность кандидата на вербовку к установлению постоянных деловых отношений, совокупность всех мотивов, жизненных обстоятельств и особенностей характера будущего агента, которые делают для него принципиально возможным установление отношений с разведывательным органом.

Версия – одно из нескольких возможных, отличительное от других, объяснение или толкование какого-либо факта, явления, события. Предмет версий – отдельные единичные явления и факты, порой весьма незначительные. Основное отличие гипотезы от версии в том, что гипотеза направлена на объяснение значительных явлений и обосновывается длительным наблюдением, а версия – на объяснение отдельных единичных явлений и фактов.

Верификация (*лат*. vērificātiō – подтверждение истины) – в широком смысле проверка чего-либо на соответствие установленным критериям; в контексте данной книги – проверка достоверности полученных разведывательных данных.

Генеративная модель искусственного интеллекта – тип ИИ-системы, способной синтезировать текст, изображения или комбинированный медиаконтент в ответ на подсказки.

Гипотеза – обоснованное предположение, выдвигаемое для прояснения свойств и причин исследуемого явления. Гипотезы создаются для объяснения значительных событий и явлений, обосновываются длительным наблюдением.

Данные (сведения) – некий набор разрозненных атомарных фактов. Это могут быть статистические показатели, отрывочные сведения о персоналиях, хозяйствующих субъектах, в виде текстовых документов, фотографий, видео- и аудиозаписей и т. д. Преобразование и обработка данных позволяют получить информацию: например, в базах данных хранятся различные данные, а по определенному запросу система управления базой данных выдает требуемую информацию.

Дезинформация – 1) Распространение искаженных или заведомо ложных сведений для достижения пропагандистских, военных или иных целей; 2) заведомо ложное осведомление о тех или иных событиях, ставящее целью ввести кого-либо в заблуждение и тем самым помешать ему правильно разобраться в сложившейся обстановке; потеря правильных представлений о времени и пространстве; 3) способ маскировки, заключающийся в преднамеренном распространении ложных сведений об объектах, их составе и деятельности, а также имитация их деятельности в соответствии с этими сведениями; 4) проведение специальных операций и мероприятий, направленных на сокрытие от противника охраняемых секретов и введение его в заблуждение в отношении уровня ре-

шения тех или иных политических, экономических, научно-технических, военных и других проблем с целью побудить противника к таким решениям и действиям, которые были бы выгодны для дезинформирующей стороны; 5) сведения, материалы и документы, содержащие информацию, рассчитанную на введение кого-либо в заблуждение.

Дезинформационное мероприятие (сокр. ДМ) – конспиративное продвижение объекту воздействия (в данном случае оппонентам и конкурентам предприятия) специально подготовленных вымышленных сведений с целью введения их в заблуждение и побуждения к решениям и действиям, которые отвечали бы интересам руководства хозяйствующего субъекта. ДМ является одним из самых эффективных средств оперативного воздействия на противника.

Дискредитация *(*от *фр.* discréditer – подрывать доверие) – предание гласности с использованием гласных и негласных возможностей службы безопасности достоверных или субъективно толкуемых данных, направленных на подрыв авторитета, имиджа и доверия к дискредитируемому. В активных мероприятиях дискредитация используется для поддержки собственной позиции путем формирования у широких народных масс устойчивой негативной оценки оппонентов и конкурентов, выраженной особыми языковыми средствами.

Знания – систематизированные достоверные представления о предметах и явлениях действительности. Знание применяется людьми для рациональной организации своей деятельности и решения возникающих задач. Знания в виде синтезированных решений и рекомендации представляют собой конечный информационный (разведывательный) продукт.

Информация – некая совокупность данных, которые были отобраны, обработаны и систематизированы для последующего восприятия их человеком или специальными устройствами, в качестве объективного отражения фактов материального мира в процессе коммуникации.

Согласно Государственному стандарту РФ ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

По классическому определению теории информации К. Шеннона, информация – совокупность данных (сведений), полностью снимающих или уменьшающих существующую до их получения неопределенность.

Информация инсайдерская (*англ.* insider information) – подлинные сведения, которые ранее не подвергались публикации и способны существенно повлиять на цену финансовых инструментов, валют или товаров. Запрещено совершать торговые операции с финансовыми инструментами, в отношении которых у участников сделки есть инсайдерская информация.

Информационно-коммуникационные технологии (ИКТ) – различные инструменты и системы, позволяющие получать, анализировать, хранить и передавать информацию.

Информационный шум – поток неактуальной или незначимой для аналитика информации, затрудняющий поиск и обработку разведывательных данных. Выделяют два вида информационного шума:

- *непреднамеренный* – возникает случайным образом без вмешательства со стороны и рассматривается как помехи во время потребления информации;
- *преднамеренный (направленная дезинформация)* – заранее продуманные информационные потоки, которые ставят перед собой цель либо введения в заблуждение, либо целенаправленного сокрытия релевантных разведывательных данных.

Источники информации – силы и средства, имеющиеся в распоряжении службы безопасности предприятия. Это могут быть: люди, которым известны некие сведения, интересующие СБ (доверительные помощники); носители информации, попавшие в сферу оперативного интереса СБ: предметы внешнего мира и конкретные лица, хранящие следы тех или иных действий или событий, имеющих отношение к решению задач обеспечения безопасности хозяйствующего субъекта, а также сами внешние проявления таких действий или событий; сторонние организации, обладающие интересующими сведениями.

Канал получения информации – способ поступления в службу безопасности предприятия разведывательных данных либо иных оперативно значимых для нее материалов. В деятельности СБ используются следующие основные каналы получения разведывательных данных: 1) возникающий в результате непосредственного проникновения сотрудников СБ и их доверительных помощников в сферу обращения оперативно значимых сведений или контакта с лицами, обладающими к ним доступом; 2) использование технических средств обеспечения безопасности; 3) изучение открытых источников информации, а также визуальное изучение объектов оперативного интереса, осуществляемое сотрудниками СБ и их доверительными помощниками, как по месту их проживания, так и в процессе деловых и личных поездок.

Компрометация (*фр.* compromettre – подрывать репутацию) – доведение, с использованием гласных и негласных возможностей службы безопасности, до сведения конкретного заинтересованного лица (лиц), от мнения которых зависит объект воздействия, компрометирующих материалов, свидетельствующих о его неблаговидной деятельности.

Конспирация – сохранение в тайне лицами, привлекаемыми в качестве доверительных помощников, целей, содержания, форм, средств и методов решения поставленных задач, а также сведений, которые могут нанести ущерб разведывательной и контрразведывательной деятельности и ее участникам.

Модели искусственного интеллекта / машинного обучения (ИИ-модели) – математические алгоритмы, которые с помощью вклада человека (эксперта) «обучаются» на наборах данных воспроизводить решение, которое эксперт примет при анализе такого же набора данных. Обучившись воспроизводить решение эксперта, модель в дальнейшем функционирует самостоятельно, позволяя таким образом автоматизировать решение задач.

Нейросеть в машинном обучении – математическая модель, которая работает по принципу нейронной сети живого организма. В отличие от биологической нейросети, которая передает сигнал от мозга к другим органам и полностью регулирует жизнедеятельность организма, компьютерная нейросеть учится решать только ту задачу, которую ей ставит человек.

Направленная информация/дезинформация, или направленные информационные материалы (НИМ), – форма манипуляции, когда одна сторона управляет информационным потоком, передавая его другой стороне, чтобы достичь своих целей.

Неопределенность – это неполнота либо недостоверность информации об условиях исполнения решения, наличие фактора противодействия либо случайности.

Неструктурированный формат данных – данные, не имеющие четкой организации или формы, в силу чего их сложно обрабатывать с использованием традиционных аналитических методов. В качестве примера неструктурированных данных можно привести: 1) текстовые документы (не форматированные текстовые файлы, такие как документы Word, PDF, электронные письма, блоги); 2) изображения и видео (фотографии, видеозаписи, сканированные изображения и другие мультимедийные файлы); 3) аудиофайлы (звуковые записи, аудиокниги, подкасты и другие аудиофайлы); 4) данные из средств массовой коммуникации (изображения, посты и комментарии в социальных медиа).

Объект воздействия – человек или группа лиц, в отношении которых совершаются действия непосредственного активного влияния, не обязательно явного.

Оперативная информация (в сфере обеспечения безопасности) – сведения, попадающие в распоряжение службы безопасности предприятия оперативным путем, то есть в результате проведения оперативных мероприятий и выполнения разведывательных и контрразведывательных действий.

Оперативная информация (в экономической сфере) – информация, используемая в оперативном управлении предприятием и характеризующая производственные процессы в текущий (данный) период времени.

Оперативная игра – агентурно-оперативное мероприятие с использованием «подстав», легендированных организаций, перевербованной агентуры оппонентов, средств оперативной техники для выявления нелояльности персонала предприятия, дезинформирования и срыва преступных замыслов конкурентов, криминальных сообществ и отдельных лиц, вынашивающих противоправные намерения.

Оперативная комбинация – совокупность тактических приемов и действий, объединенных единым замыслом и легендой, направленных на создание искусственных условий, способствующих решению службой безопасности предприятия служебных задач в конкретных ситуациях, а также позволяющих службе безопасности осуществлять контроль за такими ситуациями, исключая действия провокационного характера.

Оперативный эксперимент – оперативно-разыскное мероприятие, состоящее в негласном изучении деятельности определенного лица в специально созданных условиях. Оперативный эксперимент проводится на основании постановления,

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru