5) информационная безопасность - понятие определяющая уровень защиты информационных ресурсов государства от внешних и внутренних угроз. Обеспечение свободы слова и свободы информации, защита информационных источников является ключевым вопросом данного компонента.

6) экологическая безопасность – понятие определяющая уровень защиты общества от природных, экологических и антропогенных факторов. В этом вопросе важным фактором является решение трансграничных экологических проблем и повышение стремления международного сообщества в содействии решения данного вопроса.

В ходе анализирования составных частей задач национальной безопасности, мы приходим к выводу что, она тесно связана с безопасностью социально-политической системы того или иного государства в целом. Для достижения своих целей, то или иное государство вступает в отношение с другим государством которое содействует или же препятствует достижению целей. Следовательно, национальная концепция безопасности государства должна создаваться с учётом существования как внешних так и внутренних угроз

Таким образом обеспечение национальной безопасности- это комплекс политических, экономических, социальных, оборонительных и правовых мер направленных на обеспечение стабильного образа жизни населения, защиты его от любых форм проявления угроз. Для защиты жизненно важных интересов государства и общества необходима целостная концепция способствующая защищать от внешних и внутренних угроз. Необходимо постоянное усовершенствование концепции с учётом современных тенденций развития.

Литература

1. Каримов И.А. Узбекистан на пороге XXI века: бўсағасида: угрозы безопасности условия и гарантии прогресса.//Безопасность и пути устойчивого развития. Том 6.- Ташкент, Издательство: «Узбекистан», 1998. С. 31-261.

2. За мир надо бороться//За безопасность и мир надо бороться.Том 10.- Ташкент, Издательство: «Узбекистан», 2002.С. 120-124.

3. Маккиндер Х. Дж. Географическая ось истории.- Полис.-1995.- № 4.

В.А. Супрыткина

ИССЛЕДОВАНИЕ МЕТОДОВ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

В современном мире, где технологии просочились во все аспекты жизни человека, информационная безопасность играет важнейшую роль. И если правительственные структуры уже давно выделили защиту информации как одно из приоритетных направлений деятельности, то население и организации част-

ного сектора во многом только сейчас начали осознавать важность применения мер безопасности. Однако даже понимая, насколько необходимо обеспечение информационной безопасности, люди не всегда правильно представляют что именно представляет из себя этот процесс.

Существует множество способов и средств защиты информации, причем особую популярность приобрели технические средства и организационные меры, применение которых действительно эффективно, но создает иллюзию того, что информация полностью защищена. С этим утверждением может поспорить любой специалист по информационной безопасности, так как даже самый тщательный подход к закрытию существующих и возможных уязвимостей не дает абсолютной гарантии безопасности системы и ее компонентов. Можно сколь угодно много времени и сил тратить на предотвращение рисков атак, сбоев и прочих нарушений конфиденциальности, целостности и доступности информации, однако остается проблема, которую невозможно закрыть. Речь идет о человеческом факторе, который в данном контексте следует интерпретировать как причину распространенности применения методов информационного воздействия.

Существует некий принцип, часто применяемый специалистами ИБ, суть которого состоит в следующем: чтобы научиться защищать, нужно научиться ломать. Иными словами, необходимо понимать логику атакующего и его методы, чтобы суметь с большей долей успеха противостоять атаке на субъект защиты. Так какие же методы информационного воздействия существуют? Каким образом можно распознать факт информационного воздействия?

Наиболее распространенным методом информационного воздействия, который находится на слуху практически каждого человека, является дезинформация. Поле деятельности обширно и охватывает как разведку и контрразведку (политическую, экономическую), так конкуренцию, что включает формирование имиджа, рейтинговых оценок. Информация попадает в открытые источники (например, в СМИ) в искаженном виде: полуправды, тщательно подогнанных фактов. Качественная дезинформация должна складываться в достоверную картину событий, чтобы не вызывать подозрений, поэтому зачастую она содержит подлинные данные, к которым «примешивается» информация, нацеленная на составление ложного мнения. Одна из форм дезинформации – белый шум. Это подача значительных размеров потока информации, среди которого невероятно сложно выделить ложные данные, потому что такой массив не поддается сортировке.

Информационный плюрализм играет значимую роль в манипулировании общественным сознанием. На данный момент существует огромное количество источников информации, что создает впечатление многообразия и возможности выбора. Однако одна только конкуренция приводит к той ситуации, при которой разнообразие сводится лишь к поверхностному отличию при подаче одной и той же информации. В итоге получаем информационную перегрузку при незначительном возрастании количества значимой информации, что в разы усложняет поиски правды и смысла.

Популярным методом также является отвлечение внимания людей на сторонний объект, который в данной конкретной ситуации не имеет значимости, но преподносится как стоящий или даже компрометирующий. Это способ сбить человека с толку или подтолкнуть его сконцентрироваться на отвлеченной теме, новости, событии.

В мире, где с каждым годом всё больше ускоряется ритм жизни, скорость передачи информации имеет огромное значение, однако этот показатель с трудом можно назвать достоинством. Различные структуры, в том числе СМИ, работают на опережение, чтобы первыми доставить информацию конечным получателям. В таких условиях недостаточно времени на проверку получаемых данных и на формирование наиболее качественного итогового материала. А у получателей недостаточно времени на ее осмысление. Поэтому скорость передачи является очень эффективным методом манипуляции, который мешает понимать и делать верные выводы о сути конкретной ситуации (или информации).

Правильным решением при целенаправленной работе с информацией является поиск ее первоначального источника, что позволяет частично отфильтровать субъективные мнения (или просто иметь в виду природу субъективности позиции), которые присущи тем или иным «поставщикам» информации. Однако порой это сделать крайне сложно и даже невозможно, когда в дело вступают такие приемы, как контролируемая утечка информации, которая подразумевает сокрытие этого самого источника. Происходит цепочка «секретных» утечек заранее сфабрикованных данных, и в конечном итоге, когда данные попадают в СМИ, маловероятно отследить все точки передачи. Однако как раз неизвестная природа этой информации в умах дотошных людей должна вызывать подозрения.

Борьбой с манипуляцией сознанием масс и отдельных индивидуумов или их групп можно заниматься во многих направлениях. В качестве примера далее будет рассмотрена информационно-аналитическая работа с одним из основных источников информации, а именно обработка материалов средств массовой информации.

На приведенной ниже схеме (Рисунок 1) описывается алгоритм работы с информацией, выпускаемой СМИ вне зависимости от вида ее представления (для удобства бумажные материалы могут заранее быть переведены в электронные). Первые три блока могут использовать как частные лица, так и сотрудники различных коммерческих структур, которых интересует достоверность предоставляемой в открытых источниках информации. Последний блок подразумевает значительные затраты времени и средств, потому используются в основном организациями.

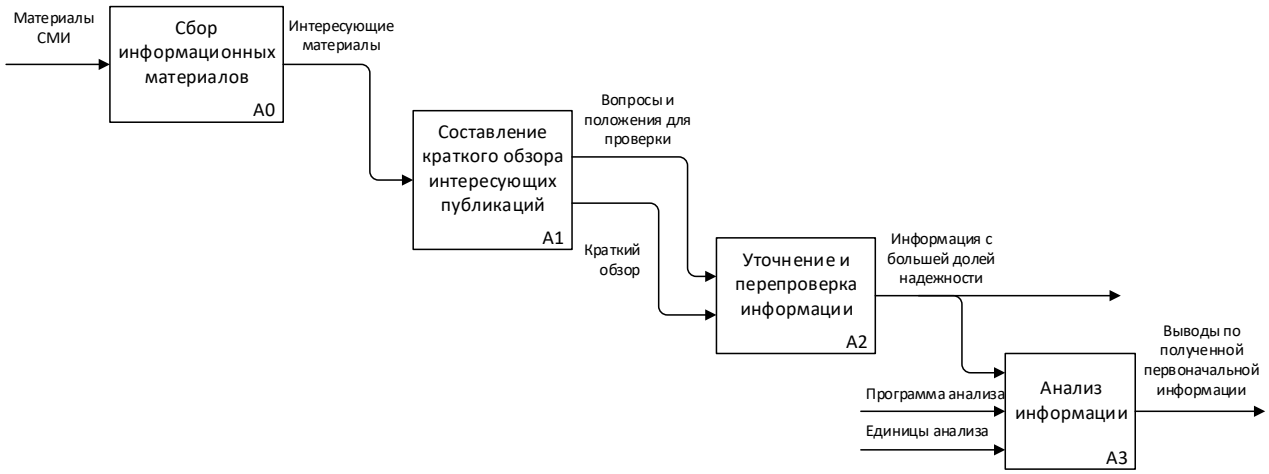

Рис. 1. Общая схема информационно-аналитического анализа СМИ

Анализ информации составляет отдельную тему для рассмотрения. Одним из вариантов аналитической обработки информации является метод контентного анализа данных, который представляет собой достаточно трудоемкий процесс. Суть его заключается в анализе содержания материалов путем выделения конкретных интересующих информационных единиц анализа (характеристик текста, отвечающих задачам исследования: например, при анализе эмоциональности текста могут выбираться языковые маркеры, которые указывают на то, что при подаче материала имеет место агрессивность). Затем в зависимости от цели исследования выявляются частотные характеристики их употребления, наличие или отсутствие определенных тем, их связь между собой и основную мысль в заранее выбранном объеме информации. Это позволяет определить первоначальный посыл и направленность материала.

Аналитическая работа может проводиться самостоятельно и с привлечением сторонних лиц. Также могут быть задействованы программные средства обработки неструктурированной информации, которых на сегодняшний момент существует огромное множество, и каждое решение имеет свой ряд достоинств и недостатков. Они используют технологию полнотекстного анализа, который имеет несколько разновидностей: прямой поиск в каждом из перебираемых файлов (AVSearch, SSScanner), поиск с индексированием с созданием собственной базы данных на основе анализируемых текстов для дальнейшего поиска (Advanced Document Server, Следопыт). Их применение помогает оптимизировать процесс анализа информационных материалов, что доступно даже просто заинтересованным лицам (правда, бесплатные или недорогостоящие продукты не обладают особым разнообразием возможностей). В связи с этим задача поиска истины в большом потоке информации имеет определенный смысл и шанс на успех.

Информационная безопасность имеет множество направлений, и не стоит уделять внимание только самым очевидным, следует использовать многоаспектный подход к защите. Проверять поступающую информацию также важно, как и защищать ее при хранении, обработке, передаче. Знать и понимать мето-

ды злоумышленника также важно, как и пытаться им противостоять. Информационно-аналитический анализ – только один из способов, который позволяет противодействовать манипуляциям сознанием, однако знание и применение его необходимо для нашей же безопасности.

Литература

1. А.И. Доронин Бизнес разведка, 5-е издание: Ось 89; Москва; 2009
2. Семёнова А.В., Корсунская М.В. Контент-анализ СМИ: проблемы и опыт применения / Под ред. В.А. Мансурова. – М.: Институт социологии РАН, 2010. – 324 с.
3. Контент-анализ публикаций СМИ [Электронный источник]. - https://studopedia.ru/14_88868_kontent-analiz-publikatsiy-smi.html.
4. Информационное воздействие: виды, средства, объекты [Электронный источник]. - https://studfiles.net/preview/1113130/page:2/.

О.Ш. Узаков

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ ГОСУДАРСТВЕННОГО СТАНДАРТА УЗБЕКИСТАНА DST2005

(Каршинский филиал Ташкентского университета
информационных технологий имени Мухаммада аль-Хоразмий)

Настоящий стандарт «Алгоритм шифрования данных» (АШД) DSt2005 представляет собой криптографический алгоритм, предназначенный для защиты электронных данных. АШД DSt2005 - симметричный блочный шифр, который используется для зашифрования и расшифрования информации. АШД DSt2005 может использовать криптографические ключи длиной 128, 256, 512 бит для зашифрования и расшифрования блоков данных длиной 128 или 256 бит.

Стандарт устанавливает единый алгоритм шифрования информации для систем обработки информации в сетях электронных вычислительных машин (ЭВМ), телекоммуникаций, отдельных вычислительных комплексах и ЭВМ и определяет правила шифрования данных.

Стандарт может быть использован для криптографической защиты данных, хранимых и передаваемых в сетях ЭВМ, телекоммуникаций, в отдельных вычислительных комплексах или в ЭВМ коммерческих организаций и предприятий для шифрования данных не являющихся под грифом (ДСП, секретно, сов. секретно, особой важности).

Ниже приведем оценку сложности АШД DSt2005, схема алгоритма шифрования данных приведена на рис. 1. для случая 128-битного блока данных.

Вначале мы имеем значение выхода из массива *Holat* выходных блоков *chiqish* по 32 бита. Восстановление входных значений массива *Holat* блоков