УДК 681.142.37; 316.32

Д.В. Ландэ, В.Н. Фурашев

WikiLeaks – начало переформатирования информационного общества?

Научно-исследовательский центр правовой информатики
Национальной академии правовых наук Украины

Проанализированны технологические аспекты реализации проекта Wikileaks и степень влияния этого проекта на сложившиеся информационные отношения на всех уровнях – глобальном, региональном, государственном и корпоративном.
Ключевые слова: информационная безопасность, информационное общество, информационные отношения, прогноз.

26 июля 2010 год Администрация Соединенных Штатов Америки заявила, что «безответственная» утечка в СМИ тысяч файлов с секретной военной информацией может представлять угрозу для безопасности страны. Речь шла о документах, опубликованных на сайте Wikileaks и перепечатанных ведущими мировыми изданиями – британской Guardian, американской New York Times и немецким журналом Spiegel.

23 октября 2010 г. сайт Wikileaks опубликовал около 400 тысяч документов, посвященных войне в Ираке. Как говорится на сайте, 391 тысяча 832 военных отчета, получившие название «Иракское досье», охватывают период с 1 января 2004 года по 31 декабря 2009 года.

В конце ноября 2010 года на сайте Wikileaks появилось более 250 тысяч писем дипломатов США.

Критики Wikileaks – преимущественно, представители военных и государственных структур обвиняют создателей портала в создании угрозы военных операций и нарушении частной жизни. Еще в 2008 году американские военные назвали WikiLeaks потенциальной угрозой безопасности.

Так что же такое «портал Wikileaks» (англ. Wiki – указатель применяемой технологии, напр. Wikipedia, Wikimedia и т.п., и leak – утечка) **? Какая направленность его информационного ресурса? Какие технологические принципы его организации и информационной поддержки?** Портал WikiLeaks был основан в декабре 2006 года и с тех пор здесь были опубликованы более миллиона секретных документов, в том числе о захоронении токсичных веществ у африканского побережья и инструкции для американских военных, работавших в тюрьме Гуантанамо на Кубе, а также пейджинговые сообщения, отправленные пользователями в Нью-Йорке и Вашингтоне 11 сентября 2001 года. При этом портал не раскрывает источники своей информации. Однако в любом случае, опубликованная на портале информация, **как правило**, расценивается как надежная.

Проект Wikileaks был представлен в Интернете в конце декабря 2006 года. Уже по названию можно понять, что сайт работает на том же движке, что и общеизвестная Wikipedia (Википедия), хотя этот выбор был обусловлен исключительно простотой редактирования, а не попыткой привлечь пользователей к наполнению сайта. Авторы проекта изначально позиционировали ресурс как сайт, на страницах которого будут публиковаться разного рода разоблачительные документы. Портал WikiLeaks.org изначально входил в систему

wikipedia.org. Теперь, очевидно, это не так. Несмотря на свое название, Wikileaks не является вики-сайтом: читатели, не обладающие соответствующим разрешением, не могут менять его содержание. После перезапуска проекта в мае 2010 года пользователи лишились возможности участвовать в обсуждении посредством функционала wiki на сайте проекта, а описание проекта на сайте было исправлено: если в 2007 году на нем говорилось, что WikiLeaks является "Википедией" без цензуры, то в 2010 году уже сообщалось, что WikiLeaks - не "Википедия", и функциональности "Википедии" у проекта нет.

С технической точки зрения WikiLeaks по идее своих создателей должна была обеспечить:

1) возможность редактирования материалов и размещения их на веб-ресурсах;

2) децентрализированное хранение данных при сохранении анонимности их владельцев;

3) многоступенчатую анонимную передачу информации таким образом, чтобы промежуточные звенья в цепи передачи информации не знали адресов отправителей и адресатов;

4) надежное шифрование информации.

Большое внимание при создании WikiLeaks было уделено защите ресурса и обеспечению анонимности источников данных. Обеспечена возможность переписки между редакторов между собой переписываются по зашифрованным каналам связи для защиты передаваемых данных от перехвата. Авторы проекта также побеспокоились о предотвращении возможного удаления данных, размещенных на ресурсе. WikiLeaks построен таким образом, чтобы после публикации контент сразу же отображался на нескольких сотен зеркал, в результате чего удалить материалы с сайта стало практически невозможно.

Соответственно, WikiLeaks базируется на использовании таких технологий (рис. 1.):

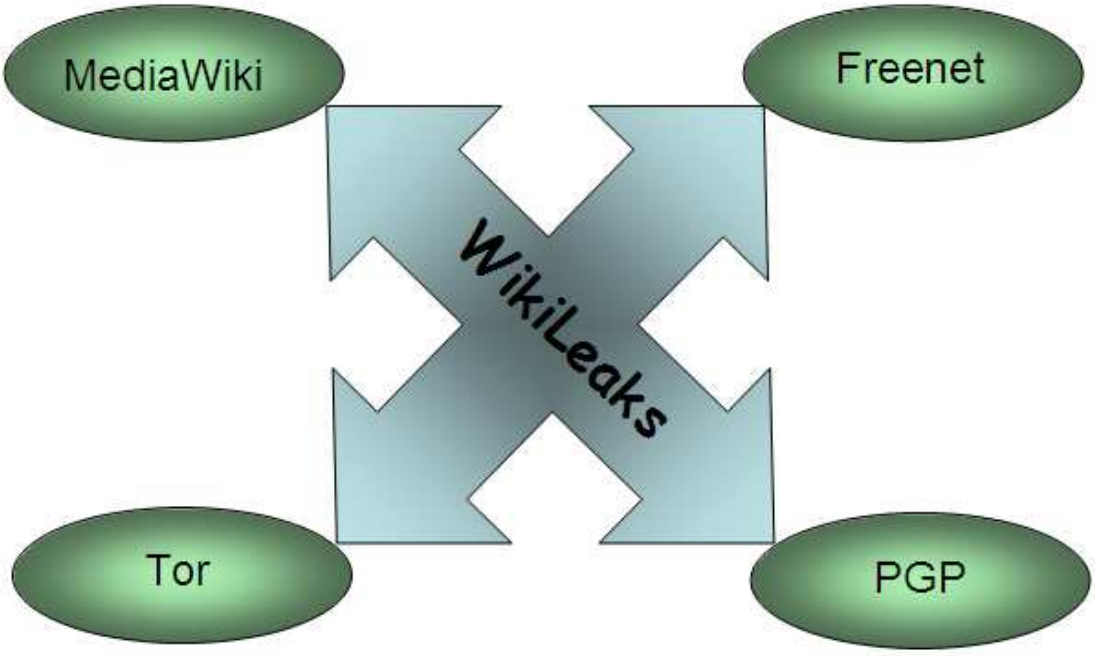

Рис. 1. Основные компоненты технологии WikiLeaks.org

1) MediaWiki (основная система управления контентом всех вики-проектов);

2) Freenet (децентрализованное анонимное хранилище данных, где никто не знает, что хранит);

3) Tor (сеть «луковой» маршрутизации);

4) PGP (от англ. аббревиатуры – довольно хорошее шифрование) – способ шифрования информации.

Краткий обзор каждой из этих технологий сделан ниже. Для навигации возможен защищенный доступ с использованием защищенного HTTPS-протокола (протокол передачи гипертекста с шифрованием).

Важное значение для любого социального сетевого проекта имеет качество, надежность и безопасность его размещения в Интернете. Первым хостинг-провайдером для WikiLeaks была компания PRQ.se, которая предоставляла хостинг с гарантией того, что размещенный сайт не будет закрыт по судебному требованию. Эта же компания размещала у себя небезызвестный файлообменный торрент-портал The Pirate Bay. В августе 2010 года WikiLeaks выбрали себе новый хостинг в дата-центре Pionen, принадлежащем Bahnhof ISP, и расположенном в подземном ядерном бункере времен Холодной войны под центром Стокгольма. Однако еще несколько месяцев часть файлов проекта хранилась на PRQ, но в ноябре 2010 года провайдер отключил сервера ресурса.

MediaWiki *(МедиаВики)* – это программный механизм управления контентом веб-сайтов, работающих по технологии «Wiki», написанный специально для WikiPedia и использующийся во многих других проектах фонда «WikiMedia», частных и государственных организациях. MediaWiki – это свободное программное обеспечение, распространяющаяся на условиях Общественной лицензии GNU.

MediaWiki написан на языке программирования PHP и для хранения данных использует реляционную базу данных (можно использовать MySQL, PostgreSQL, SQLite); поддерживает использование программ кэширования.

MediaWiki предоставляет интерфейс работы с множеством веб-страниц, разграничение прав доступа к администрированию системы, возможность обработки текста как в собственном формате, так и в форматах HTML и TeX (для формул), возможность загрузки изображений и других файлов. При этом пользователи имеют возможность добавлять собственные новые возможности и программные интерфейсы.

В MediaWiki предусмотрен специальный интерфейс прикладного программирования, обеспечивающий прямой доступ к информации из баз данных. Клиентские программы могут использовать API для авторизации, получения данных и отправки изменений. В качестве примера программ, использующих API, можно назвать библиотеку Pywikipedia для создания wiki-бота (программы для массовой загрузки сообщений в WikiPedia) и программу для внесения полуавтоматических изменений в Википедию AutoWikiBrowser.

Freenet (www.freenetproject.org) – это одноранговая сеть, предназначенная для децентрализованного распределенного хранения данных без возможности их цензуры, созданная с целью предоставить пользователям электронную свободу слова путем обеспечения их строгой анонимности. Freenet работает на основе объединения в общий фонд (пулинга) предоставленной пользователями (членами сети) своей полосы пропускания и дискового пространства своих компьютеров для публикации или получения из Freenet разного рода информации. Freenet использует разновидность маршрутизации по ключам, похожей на

распределенную хеш-таблицу, для определения местонахождения пользовательских данных.

Freenet может рассматриваться как огромное устройство хранения информации. Когда вы сохраняете файл в это устройство, вы получаете ключ, с помощью которого вы можете получить информацию обратно. Когда вы предъявляете Freenet ключ, она возвращает вам сохраненный файл (если он существует). Это устройство хранения данных распределено по всем узлам, подключенным к Freenet.

Сеть Freenet хранит данные и позволяет извлекать их, подобно тому как это реализовано в протоколе HTTP. Сеть разработана для того, чтобы сохранять высокую живучесть при полной анонимности и децентрализации всех внутренних процессов по всей сети. Система не имеет центральных серверов и не находится под контролем каких-либо персон или организаций. Даже создатели Freenet не имеют никакого контроля над всей системой. Сохраненная информация шифруется и распространяется по всем компьютерам, участвующим в сети во всем мире, которые анонимны, в большом количестве и постоянно обмениваются информацией. При этом достаточно сложно определить, какой участник хранит данный файл, так как содержимое каждого файла зашифровано и может быть разбито на части, которые распределяются между множеством различных компьютеров.

Tor *(The Onion Router)* – свободное программное обеспечение для реализации так называемой «луковой маршрутизации» – гибридной анонимной сети. Это система, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Tor – это анонимная сеть, предоставляющая передачу данных в зашифрованном виде.

Система Tor была создана в исследовательской лаборатории Военно-морских сил США по федеральному заказу. В 2002 году эту разработку решили рассекретить, а исходные коды были переданы независимым разработчикам, которые создали клиентское программное обеспечение и опубликовали исходный код под свободной лицензией, чтобы все желающие могли проверить его на отсутствие ошибок и программных закладок.

С помощью Tor пользователи могут сохранять анонимность при посещении веб-сайтов, публикации материалов, отправке сообщений и при работе с другими приложениями, использующими протоколы Интернета. Безопасность трафика обеспечивается за счет использования распределенной сети серверов (так называемых нодов) – «многослойных маршрутизаторов» (onion routers). Технология *Tor* также обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только анонимность пользователя, но также конфиденциальность бизнес-данных, деловых контактов и др.

О поддержке проекта объявила известная организация по защите гражданских свобод Electronic Frontier Foundation, которая начала активно пропагандировать новую систему и прилагать значительные усилия для максимального расширения сети своих узлов (нодов). Главный сервер проекта существует при поддержке данной организации. По состоянию на март 2010 года сеть включает более 2100 нодов.

Область применения Tor: Частные лица используют Tor для защиты неприкосновенности частной жизни и получения доступа к информации, заблокированной интернет-цензурой. Правоохранительные органы используют Tor для скрытого посещения веб-сайтов, чтобы не оставлять при этом IP-адреса

своих учреждений в логах соответствующих веб-серверов, а также для обеспечения безопасности сотрудников при проведении спецопераций. Военные используют Tor для сбора сведений из открытых источников.

Пользователи сети Tor запускают onion-proxy на своей машине, данное программное обеспечение подключается к серверам Tor, периодически образуя *виртуальную цепочку* сквозь сеть Tor, которая использует криптографию многоуровневым способом (или многослойным: аналогия с луком или русской «матрешкой»). Каждый пакет, попадающий в систему, проходит через три различных прокси-сервера (узла), которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго, и, в конце концов, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (аналогия с тем, как чистят луковицу) и узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом.

Внутри сети Tor трафик перенаправляется от одного маршрутизатора к другому и окончательно достигает *точки выхода*, из которой чистый (нешифрованный) пакет уже доходит до изначального адреса получателя (сервера). Трафик от получателя (сервера) обратно направляется в *точку выхода* сети Tor.

Обеспечивая анонимность клиентов, Tor также может обеспечивать анонимность для серверов. Используя сеть Tor, возможно использовать сервер таким образом, что его местонахождение в сети будет неизвестно. Конечно, для доступа к скрытым службам Tor должен также использоваться и на стороне клиента.

Таким образом, анонимная луковая маршрутизация – это когда звенья цепочки передачи данных не знают, кто инициирует передачу информации, и кто ее примет в итоге. Таким образом эти звенья снимают с себя ответственность за выдачу конечных узлов, потому что сделать это они просто не могут.

Wikipedia блокирует создание учетных записей пользователей, а также редактирование статей при использовании Tor. Большинство узлов Tor, работающих как ретрансляторы, занесены в черный список IP-адресов с формулировкой «открытый прокси». Сделано это с целью воспрепятствования вандализму – анонимному разрушению страниц.

PGP (*Pretty Good Privacy*) – компьютерная программа, так же библиотека функций, позволяющая выполнять операции шифрования (кодирования) и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде. Первоначально разработана Филиппом Циммерманном в 1991 году.

PGP имеет множество реализаций, совместимых между собой и рядом других программ (GnuPG, FileCrypt и др.) благодаря стандарту OpenPGP (RFC 4880), но имеющих разный набор функциональных возможностей.

На данный момент не известно ни одного способа взломать шифрование PGP при помощи полного перебора или уязвимости криптоалгоритма. Кроме защиты данных, передаваемых по сети, PGP позволяет шифровать запоминающие устройства, например, жесткие диски.

Криптографическая стойкость PGP основана на предположении, что используемые алгоритмы устойчивы к криптоанализу на современном оборудовании. Например, в оригинальной версии PGP для шифрования ключей сессии использовался алгоритм RSA, основанный на использовании

односторонней функции (факторизация). В PGP версии 2 также использовался алгоритм IDEA, в следующих версиях были добавлены дополнительные алгоритмы шифрования. Ни у одного используемого алгоритма нет известных уязвимостей.

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причем каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов.

PGP поддерживает аутентификацию и проверку целостности посредством цифровой подписи. По умолчанию она используется совместно с шифрованием, но также может быть применена и к открытому тексту. Отправитель использует PGP для создания подписи алгоритмами создания электронной цифровой подписи RSA или DSA. При этом сначала создается хеш открытого текста (также известный как дайджест), затем – цифровая подпись хеша при помощи закрытого ключа отправителя.

В целях уменьшения объема сообщений и файлов и, возможно, для затруднения криптоанализа PGP производит сжатие данных перед шифрованием.

PGP изначально разрабатывалась для шифрования электронной почты на стороне клиента, но с 2002 года включает также шифрование жестких дисков переносных компьютеров, файлов и папок, сессий программ мгновенного обмена сообщениям, пакетной передачи файлов, защиту файлов и папок на сетевых хранилищах, шифрования HTTP запросов и ответов на стороне сервера и клиента.

Из этого, даже краткого, обзора технологического построения и реализации проекта Wikileaks можно сделать некоторые **выводы**:

1. Можно констатировать, что первоначальные цели, которые были задекларированы на начальном этапе разработки и реализации проекта Wikileaks, – достигнуты.

Более миллиона уже опубликованных на портале Wikileaks секретных материалов (сколько будет еще опубликовано – никому не известно, даже «родителями») привлекли самое пристальное внимание мировой общественности, в первую очередь, других интернет-ресурсов.

В качестве примера возрастающего интереса к контенту портала Wikileaks и взаимосвязи этого интереса с новыми «утечками» информации можно привести динамику публикаций с ссылками на Wikileaks на веб-страницах RUNet и UANet (рис. 2 и 3), которые были получены с помощью разработанной в ИЦ ElVisti системы контент-мониторинга новостей InfoStream [1]. Динамика рассчитывалась начиная с 1 января 2007 г., практически с того момента, когда появились первые публикации о деятельности Wikileaks, до середины декабря 2010 г.

Необходимо отметить, что с целью визуализации и анализа временных рядов, связанных с публикациями в информационном пространстве сети Интернет известен метод дисперсионного анализа, предназначенный для анализа и визуализации состояния временных рядов интенсивности публикаций по определенной тематике – ΔL-анализ [2]. ΔL-метод применяется для реальных временных рядов, например тех, которые отражают интенсивность публикаций данной тематики в Интернете. На рис. 3 приведена ΔL-диаграмма для рассмотренного выше временного ряда из количества публикаций сообщений за сутки на протяжении указанного периода. Светлые области на диаграмме соответствуют максимумам количества публикаций. При этом «рельефность»

диаграммы позволяет оценивать уровень этого значения, усредненный по различным значениям «окон измерения». Данный метод визуализации абсолютных отклонений ΔL, как и известный метод вейвлет-преобразований, позволяет обнаруживать единичные и нерегулярные «всплески», периодичность, резкие изменения значений количественных показателей в разные периоды времени.

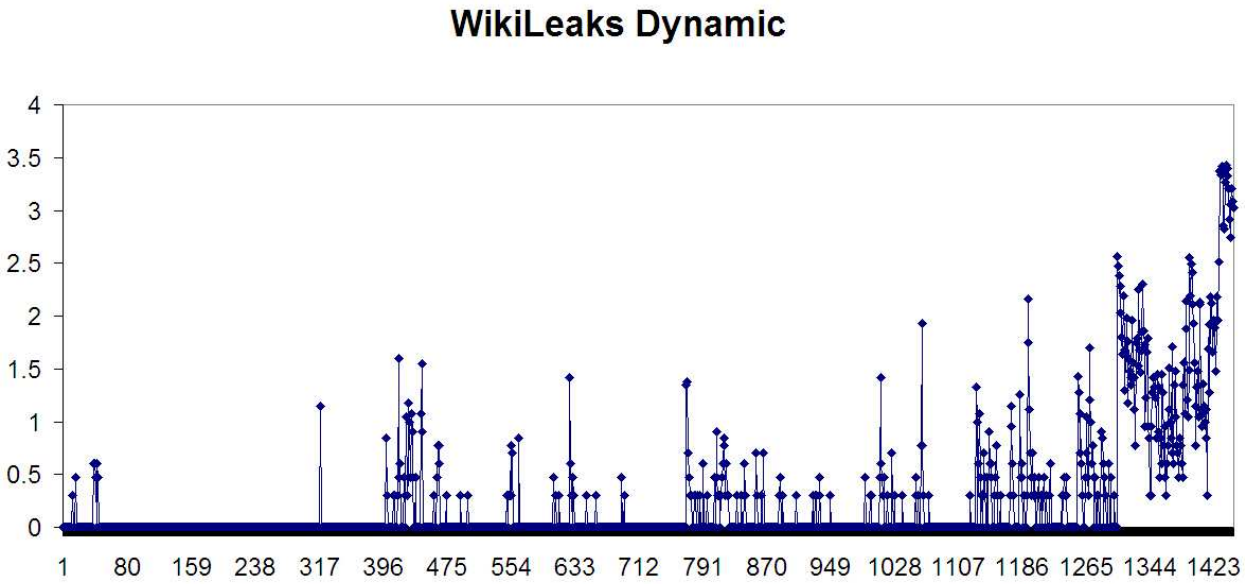

Рис. 2. Динамика публикаций в RUNet и UANet информации с контент-ресурса Wikileaks. Горизонтальная ось – порядковый номер дня, вертикальная ось – значение log(N+1), где N – количество публикаций за сутки (данные получены с помощью системы контент-мониторинга InfoStream)

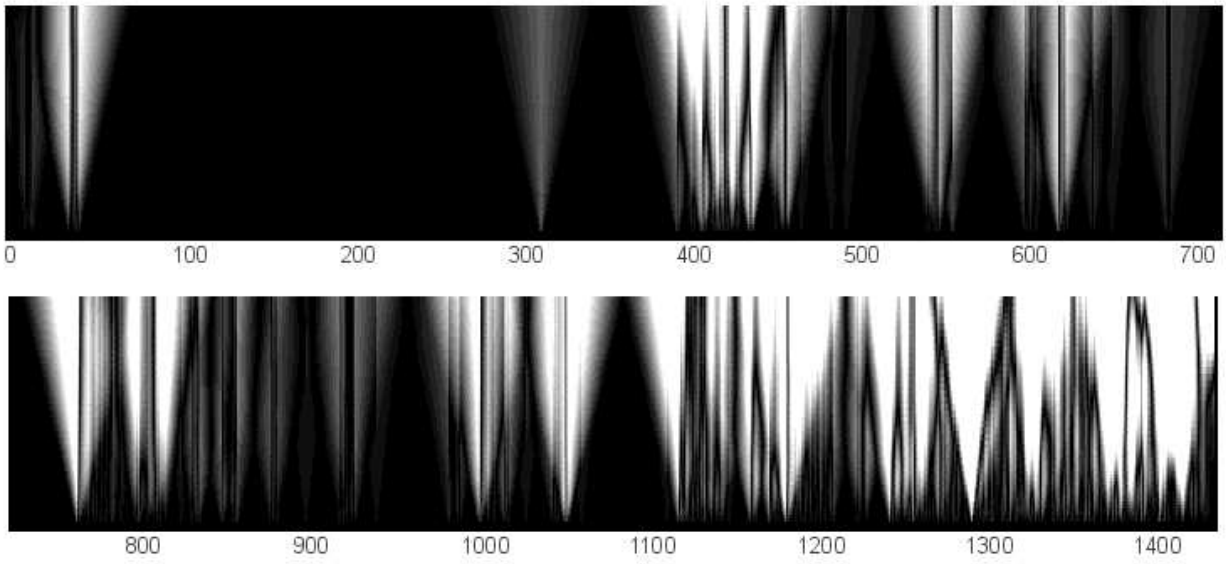

Рис. 3. ΔL-диаграмма временного ряда интенсивности публикаций о деятельности Wikileaks (ось абсцисс - дни года, ось ординат - величина окна измерений)

Еще один современный метод анализа временных рядов – R/S-анализ [3], позволил вычислить параметр Херста рассматриваемого временного ряда. Значение этого параметра, равное приблизительно 0,65 свидетельствует о таком свойстве, как персистентность, т.е. корреляционной зависимости последующих и предыдущих значений. Это дает возможность прогнозировать (чисто математически, без учета реальных событий, например, ареста или возможного исчезновения Ассанжа) то, что тенденции поведения временного ряда интенсивности публикаций будут сохраняться.

2. Вероятно впервые за всю историю существования человечества, за сравнительно короткий период времени, произошла столь массированная «утечка» и опубликование в общедоступных источниках информации «закрытой» и конфиденциальной информации.

3. Успешная реализация проекта Wikileaks, в методологическом и практическом аспектах, будет иметь далеко идущие последствия в силу достаточно надежного (на сегодняшний день) обеспечения анонимности источников информации.

Как выше было уже сказано, WikiLeaks – букет технологий:

- Freenet – децентрализованное анонимное хранилище данных, где никто не знает, что хранит.
- PGP (от англ. довольно хорошее шифрование) – способ шифрования информации.
- Tor – сеть луковой маршрутизации (когда звенья цепочки передачи данных не знают, кто инициирует передачу информации, и кто ее примет в итоге). Итак, лики через луковую сеть на Look At Me!

Очень важным является и то, что авторы проекта с самого начала побеспокоились о возможном удалении данных с сайта. Создатели WikiLeaks постарались его построить таким образом, чтобы после публикации контент сразу же отображался на нескольких сотен копий-зеркал, в результате чего удалить материалы с сайта стало практически невозможно (в настоящее время WikiLeaks зеркалируется на 2174 сайтах).

4. На сегодня пока отсутствуют эффективные технические и технологические средства противоборства с порталом Wikileaks.

Пока основными средствами противоборства являются административные и судебные мероприятия, а также организация и осуществление хакерских атак на портал Wikileaks.

Власти разных государств в разное время предлагали заблокировать деятельность WikiLeaks или хотя бы закрыть доступ к сайту для пользователей. В 2007 году сайт был заблокирован в КНР, а в 2010 году - в Таиланде. Также планировали запретить доступ к сайту австралийские власти: прежде на WikiLeaks был опубликован список интернет-ресурсов, преимущественно, порнографического содержания, которые правительство потребовало заблокировать для всех пользователей страны. О намерениях добиться блокировки WikiLeaks говорили и в Пентагоне.

По решению суда Калифорнии, в понедельник 18 февраля 2008 года, по сообщению BBC News, был закрыт сайт Wikileaks.org, на котором публиковались правительственные и корпоративные документы. Такой вердикт был вынесен судом в результате рассмотрения иска швейцарского банка Julius Baer. Исковое заявление было подано Julius Baer после того, как на сайте Wikileaks.org

появились "несколько сотен" документов, касающихся оффшорной деятельности банка.

В марте 2008 года австралийская комиссия по средствам массовой информации и коммуникациям (ACMA), по сообщениям сообщает The Sydney Morning Herald, включила в черный список сайтов, доступ на которые должны будут блокировать провайдеры страны, несколько страниц ресурса WikiLeaks.

После опубликования конфиденциальных американских документов, 28 ноября 2010 года сайт WikiLeaks подвергся хакерской атаке. Сайт некоторое время был недоступен пользователям. Содержатели сайта назвали причину неполадок DDoS-атакой.

Сразу после обнародования каблограмм, которыми правительство обменивалось с посольствами США в других странах Amazon перестал предоставлять хостинг сайту WikiLeaks. 4 декабря платежная система PayPal заморозила учетную запись WikiLeaks Впоследствии были заблокированы переводы через системы VISA и MasterCard.

И этот перечень можно продолжать. Но, что интересно, те же Соединенные Штаты Америки, которые ополчились на Ассанжа, почему-то молчат, по каким каналам его сайт получил информацию. Если ему помогли хакеры, продажные клерки или плохие сотрудники компьютерных подразделений, которые оставили уязвимости в базах данных, так и надо искать и привлекать этих людей, а не того, кто опубликовал документы Да, по логике тот, кто доставил информацию, тот и виноват.

Но проблема в том, что сегодня уязвима любая информация на электронных носителях, включая секретные серверы и платежные карточки. Это следствие скачкообразного развития информационной сферы. Защитные технологии сильно отстали. Обозы к авангарду подтягиваются значительно позже.

5. С появлением портала Wikileaks значительно увеличилось влияние Internet-пространства на практически все стороны жизнедеятельности как отдельно взятой страны, так всего мирового сообщества.

Справедливости ради, необходимо отметить, что с самого начала реализации проекта Wikileaks его создатели ставили задачу размещения не только разнообразной политической или закрытой правительственной информации, но и любых других данных, которые по каким-то причинам скрываются, но должны быть доступны общественности. И это им удалось.

Следует ожидать стремительного появления «последователей» этого Internet-ресурса и, в первую очередь, на региональных уровнях, тем более, что Wikileaks - не первый онлайновый проект подобного рода. Довольно давно в Сети существуют похожие сайты Cryptome и The Smoking Gun. 6 декабря 2010 года Пиратская партия России запустила родственный проект в зоне .рф. И это только начало. Единственное, что может сдерживать этот процесс – финансовое обеспечение.

Но это «усиление» имеет как положительные, так и отрицательные стороны. С одной стороны, сделан очень серьёзный шаг в направлении контроля деятельности политиков, представителей силовых структур, финансовых магнатов общественностью, обществом. А с другой стороны, кто поручится, что вслед за сливом с Wikileaks или ему подобных веб-ресурсов не последует череда аналогичных правдоподобных, но уже целенаправленных сфабрикованных потоков? Никто. Подобным способом вполне может быть вброшена любая

информация, в том числе и «должным образом направленная и выверенная». И многие поверят. А за фальшьсливом могут последовать и конкретные действия в геополитике, региональной и государственной политике или отдельных их аспектах.

6. Следует ожидать ускорения качественно нового развития информационных технологий, прежде всего о областях обеспечения общедоступности информации, невзирая на всякого рода «грифы», обеспечения защиты «закрытой» и конфиденциальной информации от возможных «утечек» и, тем более, массового распространения.

Эта «борьба» будет осуществляться на законодательном, технико-технологическом и административных уровнях.

7. И, пожалуй, самый **главный вывод:** ***мировое сообщество вплотную приблизилось к построению качественно нового информационного пространства, информационных взаимоотношений в которых границы «закрытости», «секретности», «конфиденциальности» информации существенно сужаются.***

Список литературы

[1] Ланде Д.В., Фурашев В.М., Григор'єв О.М. Програмно-апаратний комплекс інформаційної підтримки прийняття рішень. - К.: Іжиніринг, 2006. - 48 с.
[2] Ландэ Д.В., Снарский А.А. Динамика отклонения элементов ряда измерений от локальных линейных аппроксимаций // Реєстрація, зберігання і оброб. даних. - 2009. - Т. 11, № 1. - С. 27-32.
[3] Ландэ Д.В. Фрактальные свойства тематических информационных потоков из Интернет // Реєстрація, зберігання і оброб. даних. – 2006. – Т. 8, № 2. – С. 93–99.

Рецензент: д.т.н., професор, Заслужений діяч науки і техніки України І.Ф. Бінько

Поступила в редакцию 05.01.11

Wiki Leaks – початок переформатування інформаційного суспільства?

Проаналізовано технологічні аспекти реалізації проекту Wikileaks ы ступень впливу цього проекту на інформаційні віднослення, які склалися, на всіх рівнях – глобальному, регіональному, державному та корпоративному,

Ключові слова: інформаційна безпека, інформаційне суспільство, інформаційні відносини, прогнозування.

The beginning of an information society reformatting?

Technological aspects of realization of project Wikileaks and degree of influence of this project on developed information relations at all levels – global, regional, state and corporate are analyzed.

Keywords: information security, informationsociety, information relations, the forecast.