СОЦИАЛНИТЕ МРЕЖИ В ПРАВИТЕЛСТВЕНАТА ПОЛИТИКА ЗА СИГУРНОСТ

проф. дин инж. Йордан Начев
УниБИТ

SOCIAL NETWORKS IN GOVERNMENT SECURITY POLICY

Prof. Eng. Yordan Natchev D.Sc.
SULSIT

Анотация: *В статията се изследват възможностите на социалните мрежи за тотален контрол на обществото и в каква степен това се използва от националните разузнавателни структури. Авторът анализира опитът на водещи в това отношение държави, каквито са САЩ и Руската Федерация. Отбелязани са някои специфични особености в дейността на специалните служби на Руската Федерация и тези на разузнавателната общност на САЩ. Може да се направи извод, че секретните служби разполагат с необходимата техника и имат възможност без ограничение да проследяват комуникациите по социалните мрежи, които засягат обикновените ползватели.*

Ключови думи: *национална сигурност, специални служби, социални мрежи.*

Abstract: *This article discusses the possibilities of social networks for population control in order to optimize state security policy. The author analyzes the experience of leading countries in that respect, such as the United States and the Russian Federation. Also there are indicated some features peculiar to the activities of the special services of the Russian Federation and those of the US intelligence community. It can be concluded that the secret services today are able to monitor huge volumes of data that are transmitted by social networks and are affecting ordinary citizens.*

Key words: *national security special services, social networking.*

1. Официална държавна политика

Днес сигурността на кибер пространството се третира като приоритетно направление за гарантиране на националната сигурност. Това проличава от официално декларираната държавна политика, която две от водещите световни военни сили провеждат през последните години.

На 24 юли 2013 г. руският президент Владимир Путин подписа указ в който се формулират „Основите на държавната политика на Русия в областта на международната информационна сигурност за периода до 2020 година”.[1] Посочват се възгледите на Русия по проблемите на международната информационна сигурност и се определят векторите на активност на Москва в тази сфера. Преценява се, че това ще помогне за активизиране на руския подход по въпросите на киберсигурността на международната арена и в същото време ще подобри взаимодействието на заинтересова-

ните ведомства и организации в страната. В документа се определят четири главни киберзаплахи за Русия.

- използване на информационно-комуникационните технологии като информационно оръжие за военно-политически цели;
- използване от терористи на такива технологии;
- незаконен достъп до компютърна информация, създаване и разпространение на вредни програми и
- използване на интернет-технологии за намеса във вътрешните работи на държавите, нарушение на обществения ред и пропаганда на идеи, подстрекаващи към насилие.

Три години по-късно (февруари 2016 г.), по време на заседание на федералната служба за сигурност, руският президент поиска от ФСБ да повиши нивото на защита на информационно-комуникационните ресурси на държавните агенции. Той информира, че през последната година срещу официални сайтове са били извършени повече от 24 млн. кибер атаки. В Министерство на отбраната на РФ сега активно се създава аналог на американското киберкомандване.

През януари 2008 г. американският президент Джордж Буш задължи да се изпълняват препоръките по обслужване на киберполитиката, определена от Всеобщата национална инициатива за киберсигурност (Comprehensive National Cybersecurity Initiative – CNCI) съобразно президентската директива за националната сигурност от януари 2008 г.[2] Настоящият президент Обама определи киберсигурността като едно от най-сериозните икономически и национални предизвикателства за американската нация. Според Обама CNCI и свързаните с нея дейности са ключов момент за съвременната американска стратегия по сигурността на киберпространството. През май 2009 г. президентът на САЩ прие препоръки към политиката на сигурност на киберпространството и избра координатор по дейността, който има редовен достъп до него.[3] Понастоящем CNCI обхваща поредица от взаимно подпомагащи се инициативи, които спомагат за осигуряване киберпространството на САЩ.

В съответствие с приетото законодателство, Националната агенция за сигурност (NSA) на САЩ изгражда американската политика за сигурност върху предпоставката, че наблюдението и контролът на населението в собствената страна има жизнено важно значение за националната сигурност. Отчита се, че новият дигитален свят на глобалните мрежи с кодирана комуникация изисква качествени промени в американската стратегия на проследяване. Целта е посредством тотално наблюдение на населението да може предварително придобитата информация да се използва за разкриване на потенциални опасности и своевременно идентифициране на подозрителни лица.

По време на срещата на Г-8 В средата на 2013 г. президентите на РФ и САЩ Владимир Путин и Барак Обама подписаха споразумение за създаването на комуникационна връзка, чрез която да се обменя информация за компютърни инциденти, застрашаващи националната сигурност. Предвижда се предприемане на общи законодателни стъпки с цел подобряване на киберсигурността.

Според в. „Сънди таймс", английското правителство отделя 3 млрд. долара за киберсигурност за защита от кибер-атаки и за по-активно противодействие на заплахите, идващи от Китай и Русия. Планира се да бъдат наети 300 експерти, като през следващите пет години годишно ще се харчат над $600 млн. за инициативата.

Цитираните документи определят насоките на официалната правителствена политика за контрол на кибер пространството. В тях се обхващат въпросите, отнасящи се до сигурността на държавата в стремежа й да отговори адекватно на враждебна чужда политика в тази насока на нападение. Съвсем различно стоят въпросите, засягащи сигурността на личното пространство на потребителите на социалните мрежи.

2. Неофициален контрол върху социалните мрежи

Преди години разузнавателните структури полагаха големи усилия за да изготвят досието на конкретна личност. Днес в ерата на информационните технологии това се улеснява много, поради използването на такива социални мрежи като *LinkedIn*, *Feisbuk, а също* и до голяма степен поради невежеството на хората. В тях се събира информация която позволява да се открояят и систематизират професионалните взаимовръзки на потребителите, сферите на взаимодействие, интересите и кръговете на общуване, както и множество други данни, засягащи личния живот на гражданите. Разполагането с такава информация е от национално значение за сигурността на държавата.

Докато класическите средства за масова информация относително лесно могат да бъдат контролирани от властта посредством лицензиране, финансиране, кадрови подбор и негласна цензура, нещата със социалните мрежи не стоят така. В тях не може да се закрие хостинг, който се намира зад граница, или да се премахне домейн, законно регистриран на частно име. Тези особености заставят спецслужбите да насочват все повече усилия в прилагане на средства за контрол върху интернет изданията, сайтовете и форумите. До каква степен контролът върху потребителите на социалните мрежи може да се осъществява от държавните институции в системата за сигурност проличава от практиката на две водещи в това отношение държави – Руската Федерация и САЩ.

Русия. При провеждане на „Втората Московска международна младежка конференция на творческите и политически лидери на Русия на бъдещето” през ноември 2006 г. интернет беше определен като една от най-важните възможности за бъдеща политическа дейност. В конференцията взеха участие политици, политолози и представители на младежки политически и граждански организации от цяла Русия и страните от нейната „близка чужбина”.

По време на заседанията, повод за скандал станаха основните преимущества на дейността в мрежата, каквито са лесната достъпност и свободата на словото. Скандалът беше предизвикан от предоставяне на правата за обслужване на кирилица на сайта Livejournal.com. от американската компания Six Apart на руската „Суп”. След тази сделка част от ползвателите на Livejournal заплашиха, че ще го напуснат, поради съмнения за неправомерно разпространение на информацията и възможност тя да бъде използвана срещу авторите. Представителят на компания „Суп” Антон Носик отговори на тези съмнения, посочвайки невъзможността в Русия да се гарантира личното участие в Интернет. Според него ФСБ контролира целия входящ и изходящ трафик на ползвателите на интернет.[4]

Центърът за информационна сигурност към Службата за контраразузнаване на Руската Федерация (Центр информационной безопасности – ЦИБ ФСБ) взима решение до какви материали трябва да се премахне достъп в Мрежата. За тази цел ЦИБ използва специални търсещи информационни аналитични системи, създадени от руските програмисти. През 2010 г. Центърът обяви конкурс за изготвяне на програмен продукт с цена 450 хил. рубли, като в договора се обяснява, че трябва да се разработи информационно аналитична система „Семантичен архив” за компанията „Аналитични бизнес решения”. „Семантичен архив” и подобни на нея системи са програмни

продукти, които днес се използват от руските специални служби и МВР за мониторинг на откритите СМО и интернет, включително блогосферата и социалните мрежи. В средата на 2000 г. ФСБ и МВР започнаха масово изкупуване на такива системи.[5[

Един от начините за контрол на дейността в социалните мрежи е забраната. Пример в това отношение може да се даде с развлекателната социална мрежа odnoklassniki.ru в която общуват приятели с фото и видео материали, филми сериали, музика, игри и групи по интереси. Федералната служба за сигурност (Федеральная служба безопасности – ФСБ) определи odnoklassniki.ru като сериозна заплаха за държавата и този сайт с 10 милиона посетители беше забранен. Оказа се, че с такава огромна по количество и добре систематизирана информация с данни по градове, учебни центрове, предприятия, войскови части, лични данни за руските граждани с фотографии и други подробности няма дори националното контраразузнаване.[6]

Категоричното мнение на специалистите е, че информацията от сайта odnoklassniki.ru е идеално средство за вербовка на чужда агентура. В него се съдържат лични и професионални данни, пресичащи се по смислови направления, интереси и връзки както с отделни лица, така и с цели групи. Подобна информация може да послужи също за криминални цели. По данни на ФСБ, собственост на odnoklassniki.ru е немското външно разузнаване (Bundesnachrichtendienst – BND), което е заплатило на създателите баснословна сума. Подобна сделка за 2 млн. долара BND е сключило и със сътрудник на банката на графство Лихтенщайн.[7]

Когато не може да се прилага забрана, усилията на специалните служби се насочват към убеждение в обратна посока на излъчената информация, или замърсяване на източника. В това отношение руските спецслужби разполагат с отлично подготвени специалисти за прилагане и на двата способа. Замърсители на форуми най-често са офицери от разузнаването и контраразузнаването, завербувани от тях секретни сътрудници срещу заплащане, недоволни системни администратори и дори приказливи посетители, на които им е скучно и просто се забавляват.

Според специалистите, форумите в интернет могат да бъдат контролирани и дори разрушени с прилагане на множество методи.[8] Някои от публикуваните документи разясняват част от шпионските похвати, използвани от ФСБ на Руската Федерация, Националната агенция за сигурност *(National Security Agency – NSA)* на САЩ и Английското Управление за правителствени връзки (Government Communications Headquarters – GCHQ)**.** В тях могат да се проследят способите за получаване на скрит достъп до изчислителната техника и социалните мрежи, както и възможностите за радиоелектронно разузнаване на мобилните връзки и оборудването на наблюдение на мрежата.[9]

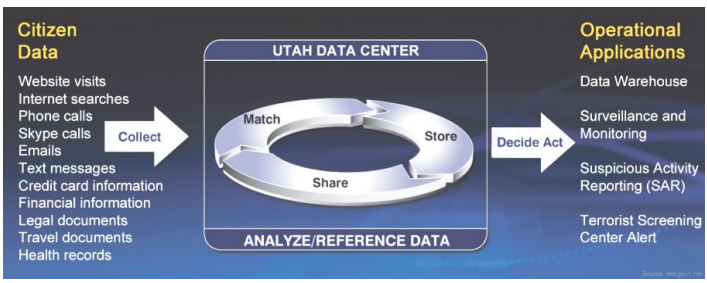
Американската *NSA* изразходва ежегодно около 300 млн. долара за възможност скрито да влияе на процесите по разработка на продуктите на компаниите. Сътрудници на английското GCHQ работят над възможността да разбиват зашифрования трафик на доставчиците на интернет услуги Hotmail, Google, Yahoo и Facebook.

САЩ. Стремежът на американските специални служби е те предварително да разполагат с информация за всеки жител на САЩ. Според тях, това ще позволи своевременно да се идентифицира подозрителната личност, което ще позволи да се действа изпреварващо. Правната основа за подобни действия почива на публикувания през 2001 г. от NSA секретен доклад Transition 2001, който определя стратегията в разузнавателната политика на американското правителство през XXI век.[10] За да изпълни поставените задачи Агенцията създава необходимите центрове и инсталира филтри в структурите на Интернет и телекомуникационни компании с което ги прави партньори за събиране на информация.

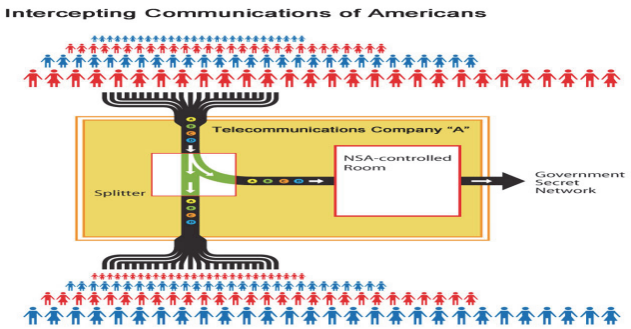
Една от специализираните структури за защита на американската нация е Центърът за придобиване на информация Утах (Utah Data Center). Той е проектиран за да оказва помощ на Разузнавателната общност (Intelligence Community – IC) на САЩ в дейността ѝ по придобиване на информация за населението. Какви данни за гражданите се събират и къде отива събраната информация се вижда от официалния сайт на Центъра.[11] (Фиг. 1)

Ето част от информацията, която се събира за ползвателите на социалните мрежи:

1. посетени адреси	2. социална активност по Фейсбук, Туитер и др.
3. шофьорски права	4. гледани или записани филми
5. активност по различни блогове	6. гледани или изпратени снимки
7. финансова информация	8. движение по кредитни и дебитни карти
9. пътувания по метрото	10. гледани и записани филми по телевизия
11. задържане от службите на реда	12. лицево разпознаване от камери за наблюдение
13. изпратени и получени и-мейли	14. изпратени и получени текстови съобщения
15. трансакции онлайн	16. записани приложения в мобилните телефони
17. билети за пътуване	18. локализиране на мобилни телефони
19. гледане видео по Скайп	20. търсене или обаждания по мрежата
21. здравна картина и образование	



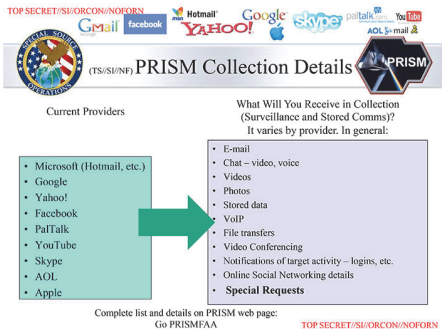
Фиг. 1. Центърът за придобиване на информация (Utah Data Center) [12]

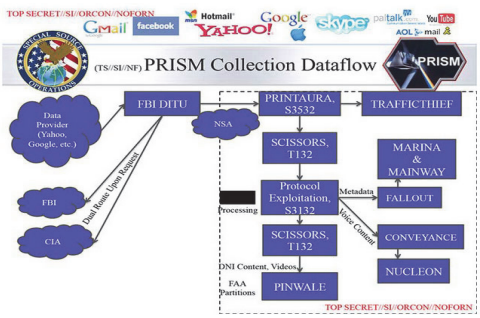


Фиг. 2. Схема на NSA за прихващане на комуникациите

Националната агенция за сигурност (NSA) има станции за прехващане на информацията в ключови места в цялата страна. Те са разположени в подходящи сгради без прозорци, които са собственост на големите телекомуникационни компании и контролират потока на националния интернет трафик. Фиброоптични сплитери препращат информацията от трафика за обработка в станции на Агенцията, както е показано на фигурата. Фиг. 2.

След 2007 г. силно засекретената американска програма Призма (PRISM program) позволи плътно да се проследяват индивидите във времето. Възможността да се провежда непрекъснато наблюдение в реално време на отделните лица дава възможност да се предвиждат техните мисли и намерения. Със своята структура Data Intercept Technology Unit (DITU) на ФБР извлича информацията от сървърите на деветте най-големи американски интернет компании – Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. По този начин NSA има директен достъп до аудио, видео, фото и и-мейли документи за всяка от тези системи. (Фиг. 3 и 4.)





Фиг. 3 и 4. Действия и възможности на програмата ПРИЗМА [13]

Друга система XKeyscore, която представлява разпространяващ Linux cluster, контролира цялата активност по интернет с помощта на повече от 700 сървъри, разположени по целия свят. XKeyscore следи в реално време всички информационни потоци от Интернет, индексира ги и съхранява в тридневна буферна база данни.

Основата на която действа XKeyscore почива на предпоставката, че хората прекарват голяма част от времето си в анонимни интернет дейности. Това дава възможност този интернет трафик да се използва за откриване на аномалиите, които произтичат от придобитата разузнавателна информация и могат да дадат индикации за последващи разследвания. Например, някой се опитва да комуникира посредством съмнителни думи или използва някакъв шифър.

През 2006 г. беше създадена друга разузнавателна програма за изследване и разширяване на техническите възможности на американската разузнавателна общност – IARPA (Intelligence Advanced Research Projects Activity). Понастоящем, с помощта на различни програми проектантите на IARPA могат да прилагат различни модели за анализ с цел да използват огромния обем вътрешна информация. Такива са програмите: [14]

- ❑ Програма Аладин (Aladdin program) извлича разузнавателна информация от видеоматериалите в интернет;
- ❑ Програма Бабел (Babel program) разработва технология за гласово разпознаване и може да осъществи ефективно търсене в огромния запис на разговори;

- Програма за проучване на знанията и тяхното разпространение (Knowledge Discovery and Dissemination – KDD) program) предоставя модерни аналитични алгоритми с които ефикасно може да се подпомогне Разузнавателната общност в създаване на виртуални центрове за анализ на дейността на разузнаването;
- Програма за социо-културно езиково съдържание (Socio-cultural Content in Language Program – SCIL). Тя разработва алгоритми, техники и технологии за разкриване на социални действия и характеристики на членовете на групите, посредством анализ на използвания език по време на комуникирането, сравнявайки приемливите социални и културни норми;
- Програма Рейнард (Reynard Program), която е изградена върху предпоставката, че характеристиките на „реалния свят" рефлектират в поведението на „виртуален свят".

От секретния бюджет на NSA за 2013 г. личи, че за Активиране на радиоразузнаването (Signals Intelligence Enabling – SIGINT) САЩ са отделили 255 млн. долара, което превишава многократно бюджетът на програмата PRISM от 20 млн. доллара годишно. През последните четири години за програмата SIGINT са изразходвани над 800 млн. долара. Една от целите на тази програма е да се вкарват слаби места в търговските системи за шифриране, които са известни само на NSA. Това позволява на разузнаването да използва данните за наблюдение. От СМО стана ясно, че компанията Майкрософт е сътрудничила с NSA при преодоляване на шифрите за електронната поща и чатовете в Outlook.com. Компанията е била принудена да се подчини на „вече съществуващите и бъдещите законни изисквания" в процеса на своите разработки.

Заключение

В зависимост от броя на посетителите и проявеният интерес, днес на практика всички форуми са под професионалното наблюдение от служители на специалните служби, които могат и да нямат отношение помежду си. Поддържайки тайни партньорски отношения с компаниите, спецслужбите залагат слаби места в шифрите, което им позволява да ги „пробиват". Често се получава така, че едни служители дори не подозират, че работят против колеги от „другата страна". Американските и британските спецслужби вкарват програми в стандартните шифри криптирани програми и устройства, внедряват агенти в IT компаниите, разбиват кодове с помощта на суперкомпютри. По този начин спецслужбите разбиват голяма част от шифрите, които милиони ползватели смятат за сигурни.

Пресен пример в това отношение е случаят със смартфона iPhone на компанията Apple. По съобщение на американското издание USA Today в края на март 2016 г., Министерство на правосъдието на САЩ отказа предявеният преди това иск към компанията Apple и помоли съдът да отмени предписанието към компанията да съдейства на властите за получаване на данни от смартфона iPhone на терориста Сайед Фарук. Преди това ФБР поиска от съда компанията да предостави програмното обезпечаване, което би позволило достъп до данните в смартфона. [15] Източник от американското правителство заяви, че методът с който ФБР вече разполага позволява на неговите специалисти да разбият системата за сигурност в смартфона iPhone без да унищожат съдържащата се в него информация. В искането към съда, Министерството на правосъдието отбелязва, че правителството вече не се нуждае от помощта на Apple, без да дава повече подробности.

Случаят засили противоречието между правителството и IT индустрията. Apple и други компании споделиха, че имат все по-остра нужда за защита на своите клиен-

ти от хакери и нежелани нарушители, докато полицията и правителствените органи предупреждават, че криптираната защита на данните затруднява разследващите органи да засичат криминални елементи и опасни терористи. [16]

В заключение можем да отбележим, че твърденията на собствениците на интернет компании, за сигурна защита на личните данни на техните ползватели не звучат убедително. Днес определено може да се твърди, че секретните служби имат възможност да следят информационния трафик по световните оптични кабели и да разбиват шифрите на потребителите. В резултат на своята дейност спецслужбите дискредитират гаранцията, която интернет компаниите дават на своите клиенти, относно защитеността на интернет записите, банковите операции и личната им информация. Както видяхме, примери в това отношение се появяват непрекъснато.

Обяснението на американската разузнавателна общност за провеждане на подобни действия е следното – „Ако няма какво да криеш, няма от какво да се страхуваш" (If You Have Nothing to Hide, You Have Nothing to Fear). [17] За оправдание на подобна политика се отбелязва, че ако силите за сигурност събират данни едва след като подозрителната личност е идентифицирана това често води до лошо разузнаване и изпускане на възможности. Правят се опити обществото да се убеди, че с помощта на тоталния контрол върху комуникациите силите за сигурност получават възможност подозрителната личност да бъде идентифицирана преди да бъде извършено престъплението.

Държавните специални служби твърдят, че разбиването на шифрите в интернет комуникациите им дава възможност да придобиват изпреварваща информация за успешна борба с тероризма. Тази постановка се използва все по-често от управляващите в различни държави. След засилването на терористичната активност в Европа и българското правителство постави на дискутиране въпроса за засилване на контрола върху гражданите за сметка на техните права. Подобна политика за намаляване на личната свобода на хората за сметка на повишена сигурност цели да оправдава всички бъдещи стъпки за тотален контрол върху обществото.

Източници:

1. http://www.scrf.gov.ru/documents/6/114.html
2. 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008.
3. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
4. http://www.svoboda.org/content/article/271857.html
5. http://best78.blogspot.bg/2011/10/blog-post_8777.html
6. http://best78.blogspot.bg/2011/10/blog-post_8777.html
7. http://midgard-info.ru/kontroliruyut-li-specsluzhby-socialnye-seti.html
8. https://megamozg.ru/post/8004/
9. http://voxdocx.com/?p=188
10. http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/
11. https://nsa.gov1.info/utah-data-center/index.html
12. https://nsa.gov1.info/utah-data-center/index.html
13. https://nsa.gov1.info/dni/prism.html
14. http://www.iarpa.gov/
15. http://techcrunch.com/2016/03/03/san-bernardino-da-claims-syed-farouks-iphone-may-house-cyber-pathogen/
16. http://news.yahoo.com/justice-department-cracks-iphone-withdraws-220719890.html
17. http://nsa.gov1.info/data/