1. АБАРОНА НОСЬБІТАЎ ІНФАРМАЦЫІ І СРОДКАЎ КАМУНІКАЦЫЯЎ

Перад тым як даваць парады, зьвязаныя з вылічальнай тэхнікай і праграмнымі тэхналёгіямі, вызначым нашыя базавыя паняткі *давер* і *надзейнасьць* у кантэксьце гэтае тэмы.

Праграма вартая даверу, калі яна дастаткова **распаўсюджаная** (маецца на ўвазе ў кампутаровым сьвеце, бо распаўсюджанасьць, напрыклад, у Буда-Кашалёве ці нават у Менску нельга ўспрымаць як сур'ёзны аргумэнт), калі яе **код даступны** для праверкі для кожнага, хто пажадае (у прафэсійнай тэрміналёгіі open-source, праграмы з адкрытым кодам), калі дыстрыбутыў (інсталяцыйны дыск) **атрыманы з вартых даверу крыніцаў**. Ня варта захапляцца скачваньнем розных цікавых праграмак з Інтэрнэту, бо існуе шмат сайтаў, дзе вы разам з крэкнутымі праграмамі атрымаеце ў дадатак пару-тройку траянаў. Калі йдзецца пра сродкі шыфраваньня і забесьпячэньня электроннае бясьпекі, пірацкі дыск, куплены з латка ці нават у краме, **не зьяўляецца вартай даверу крыніцай!** Такія праграмы трэба выладоўваць з Інтэрнэту з сайту вытворцы ці купляць праз замежныя Інтэрнэт-крамы. Інакш вы рызыкуеце нарвацца на запушчаную спэцслужбамі ці проста нягоднікамі фальшыўку, якая будзе ўтрымліваць шпігоўскія «закладкі».

Абсалютна *надзейных* праграмаў практычна не існуе, але большменш надзейнымі можна лічыць тыя, што былі праверaныя прафэсіяналамі ў галіне кампутаровай бясьпекі.

І яшчэ адна папярэдняя заўвага: усе тэхнічныя сродкі бясьпекі інфармацыі і камунікацыі мала чаго вартыя, калі ў арганізацыі пануе бязладзьдзе, адсутнічае дысцыпліна і не выконваюцца дырэктывы начальства. Калі на штаб-кватэры тусуюцца невядомыя асобы, арганізоўваюцца п'янкі і гулянкі з запрашэньнем ненадзейных, сумнеўных і патэнцыйна варожых элемэнтаў – выдаткаваныя на бясьпеку сродкі будуць простым марнатраўствам.

Як захоўваць інфармацыю на кампутары?

Працу сучаснай арганізацыі немагчыма ўявіць без шырокага выкарыстаньня кампутарнай тэхнікі. У большасьці беларускіх арганізацыяў менавіта на кампутарах, а не на паперы зьмяшчаюцца масівы

інфармацыі, у тым ліку канфідэнцыйнай, якая можа зацікавіць спэцслужбы. Часам гэтая інфармацыя можа стаць падставай для прыцягненьня да адміністрацыйнай альбо нават крымінальнай адказнасьці – у дзейнасьці беларускіх няўрадавых арганізацыяў ужо былі гэткія выпадкі.

Захоўваньне інфармацыі на кампутары больш зручнае для працы, чым захоўваньне яе ў папяровым выглядзе, а таксама ў нейкім сэнсе больш бясьпечнае. Гэта зьвязана з тым, што інфармацыю ў электронным выглядзе значна прасьцей зашыфроўваць і перазашыфроўваць, чым інфармацыю на папяровых носьбітах.

Такім чынам, галоўнае правіла, якім трэба карыстацца пры працы на кампутары, – **шыфруй!** Ваш прыватны кампутар можа быць скрадзены альбо выняты ці канфіскаваны спэцслужбамі, а таксама існуе небясьпека, што да яго могуць атрымаць доступ непажаданыя пэрсанажы. Таму абавязкова трэба карыстацца сродкамі шыфраваньня інфармацыі.

Шыфраваць можна як асобныя файлы, гэтак і цэлыя дыскі. Існуюць таксама «віртуальныя шыфраваныя дыскі» (далей ВШД) – гэта вялікія файлы, якія ўнутры сябе зьмяшчаюць у зашыфраваным выглядзе мноства іншых файлаў. Гэта падобна да zip- ці rar-архіву, адрозьненьне ў тым, што адмысловыя праграмы дазваляюць адчыніць (у кампутаровай тэрміналёгіі «змантаваць») іх так, што зь зьмесьцівам гэтых файлаў можна працаваць як з асобнымі дыскамі (ці каталёгамі), пры гэтым сыстэма аўтаматычна шыфруе тое, што вы пішаце на свой віртуальны дыск, і расшыфроўвае тое, што вам трэба прачытаць. Па заканчэньні працы вы зачыняеце (дэмантуеце) дыск – і інфармацыя становіцца недаступнай. Апісаны парадак працы карысны для няўрадавых арганізацыяў: кожны супрацоўнік мае свой зашыфраваны дыск і толькі ён ведае пароль ад гэтага дыску. Такім чынам дасягаецца дастаткова вялікая ступень карпаратыўнай бясьпекі – ня толькі праз тое, што праца кожнага з карыстальнікаў зашыфраваная і недаступная для «ворагаў», але таксама і праз тое, што супрацоўнікі ведаюць толькі свой сэгмэнт інфармацыі і ня маюць паролю для іншых ВШД. Бадай што, ВШД – адзін з аптымальных сродкаў працы зь вялікай колькасьцю важных файлаў.

Варта згадаць пра такі мэтад абароны інфармацыі, як **стэганаграфія**. Спрошчана, гэта спосаб схаваць канфідэнцыйную інфармацыю,

незаўважна ўнятрыўшы яе ў несакрэтную. Напрыклад, стэганаграфічным зьяўляецца тэкст тэлефанаваньня «Трэба ехаць у Гальшаны – бабуля ўжо нагатавала сочыва зь яблыкаў» – хто ведае, што ў гэтых бяскрыўдных словах схаванае паведамленьне «Ў падпольнай друкарні выраблены наклад улётак». Аналягічна і ў кампутаровай інфармацыі сакрэтнае паведамленьне можна прыхаваць у несакрэтным файле. З гэтай магчымасьці мае сэнс скарыстаць у выпадку, калі трэба ня проста абмежаваць доступ да інфармацыі, але зрабіць сам факт яе існаваньня таямніцай. Напрыклад, файл з дакумэнтам можна «ўплесьці» ў карцінку (здымак з рыбалкі), фільм ці музычны трэк, прычым выніковая карцінка візуальна ня будзе адрозьнівацца ад арыгінальнай, фільм можна будзе глядзець, а музыку слухаць, анічога асаблівага не заўважыўшы. Зразумела, гэты мэтад мае свае заганы. Асноўная – каб сакрэтны файл сапраўды незаўважна «расчыніўся» ў нетрах падстаўнога, памер апошняга мусіць быць сама меней у 15–20 разоў большы за памер сакрэтнага. Так што калі вы будзеце хаваць вялікія файлы, дыскавая прастора будзе выдаткоўвацца вельмі неэканомна, апроч таго, можа ўзьнікнуць праблема знайсьці падстаўны файл патрэбнага памеру.

Калі вы вырашыце пакарыстацца стэганаграфічнымі праграмамі, паклапаціцеся пра тое, каб аніхто ня выдаліў тых файлаў, у якіх таемна захоўваецца вашая інфармацыя (нехта ж можа без асаблівага клопату паставіцца, напрыклад, да музычнага файлу і выдаліць яго, каб вызваліць месца на дыску).

Паролі

Паролі для шыфраваньня – калі вы не падыдзеце да гэтага пытаньня адказна – стануць вашай праблемай.

Прыдумаць пароль для шыфравальнай праграмы – гэта сур'ёзная задача! Сучасныя сыстэмы ўзлому здольныя з высокай хуткасьцю перабіраць розныя варыянты пароляў з выкарыстаньнем слоўнікаў. Дапрыкладу, уявім грамадзкага актывіста, які дзеля прастаты ўзяў за пароль нейкае слова. Нават калі слова рэдкае – гэта пракол, бо прабегчыся па слоўніку праграма-ўзломнік зможа досыць спрытна. Хутчэй за ўсё, дастаткова будзе перабраць колькідзясят тысячаў варыянтаў, а гэта зусім няшмат для сучаснай кампутарнай тэхнікі. Дадайце да гэтага, што ў праграму могуць быць уведзеныя вашыя пэрсанальныя зьвесткі (прафэсія, любімая музыка, імёны сямейнікаў і сяброў, хобі і

г. д.), і гэта дазволіць расставіць прыярытэты і звузіць дыяпазон пошуку. Такім чынам, калі вы выкарыстоўваеце мянушку вашага сабакі ці дзень нараджэньня жонкі ў якасьці паролю – ведайце, для яго ўзлому можа хапіць некалькіх сэкундаў.

Надзейны пароль – доўгі (даўжыня залежыць ад канкрэтнага выпадку, але ў кожным разе ня менш за 8 знакаў), ніякай лёгікай ня зьвязаны з вамі і складзены з розных сымбаляў: літараў, лічбаў і спэцыяльных пазнакаў (накшталт ~ @ # &). Выкарыстоўвайце вялікія і малыя літары. Прыклад добрага паролю: Qni/u@917_GoX62. Ён нічога ня значыць, яго немагчыма вылічыць альбо падабраць з слоўніка, хіба толькі зрабіць перабор знакаў, але ж у такім разе колькасьць варыянтаў будзе занадта вялікай.

Відавочна, што надзейны пароль нялёгка запомніць, і ў выпадку, калі вам даводзіцца апэраваць мноствам складаных пароляў – хутчэй за ўсё так і будзе, – сытуацыя можа выйсьці з-пад кантролю. Многія людзі пачынаюць занатоўваць свае паролі на паперы – і гэта вельмі-вельмі кепска, бо паперкі маюць уласьцівасьць губляцца, вы можаце забыцца альбо пакінуць без нагляду свой нататнік, а ў выпадку непасрэдных рэпрэсіяў вас абшукаюць і ўсе падазроныя запісы будуць вывучаныя. Хочацца папярэдзіць, што бальшыня нібыта хітрых прыёмаў – напрыклад укласьці паперку з паролямі пад акумулятар мабільніка альбо занатаваць эсэмэскай у памяці тэлефона – насамрэч былі правальнымі яшчэ да таго, як вы іх «вынайшлі».

З гэтага тупіка існуюць тры выйсьці.

1. Захоўваць паролі ў спэцыяльнай праграме (можна парэкамэндаваць *Password Safe),* у гэтым выпадку вы цьвёрда завучваеце адзін пароль, што адкрывае доступ да праграмы, якая ў сваю чаргу падказвае вам усе астатнія.

2. Занатоўваць паролі, выкарыстоўваючы пэўны код. Які? Прыдумайце самі, і не забудзьцеся схаваць пяць сапраўдных пароляў у сотні фальшывых, запісы рабіце ў беспарадку, уздоўж і ўпоперак. Зацемім толькі, што пісаць пароль наадварот (задам наперад) – гэта ня будзе кодам, відавочна патрэбнае штосьці больш крэатыўнае.

3. Нічога не запісваць, а запамінаць з выкарыстаньнем адмысловых мнэматэхнікаў. Гэты шлях вымагае пэўнага самаўдасканаленьня.

Апошняя парада – час ад часу мяняць паролі. У гэтым выпадку, у прынцыпе, можна карыстацца праграмамі – стваральнікамі пароляў.

Рэкамэндаваныя праграмныя сродкі для шыфраваньня

Ня трэба спадзявацца на магчымасьць проста «запароліць» файлы (альбо ўключэньне кампутара) стандартнымі сродкамі – варта выкарыстоўваць спэцыяльныя крыптаграфічныя (шыфравальныя) праграмы. Няхай вас не бянтэжыць магчымае хуткае ўвядзеньне ў Беларусі адміністрацыйнай адказнасьці за парушэньне правілаў абароны інфармацыі – яна, хутчэй за ўсё, ня будзе датычыцца абароны асабістай прыватнай інфармацыі і рэальна ня будзе дзейнічаць.

Такім чынам, мы пачынаем ствараць на нашым кампутары зашыфраваны дыск.

Сродкі карыстаньня ВШД

Калі вы працуеце ў Windows XP/2000, найлепшым варыянтам – на час падрыхтоўкі нашага тэксту – зьяўляецца **TrueCrypt** – бясплатная праграма з добрай рэпутацыяй. Для старэйшых вэрсіяў Windows можна парэкамэндаваць **PGPdisk** – вэрсія 6.2 бясплатная для некамэрцыйнага карыстаньня. Гэта не апошняя вэрсія – пазьнейшыя небясплатныя, – але яна працуе і робіць усё, што неабходна. **PGP**-праграмы вельмі папулярныя, яны лічацца дастаткова надзейнымі і, што важна, «непрыкметнымі» – зашыфраванымі з дапамогаю **PGP** могуць быць ня толькі пляны палітычнай дзейнасьці, але і проста прыватная інфармацыя, якую карыстальнік палічыў патрэбным прыхаваць ад стороньняга вока. У Беларусі гэтымі праграмамі шыфраваньня карыстаюцца сотні людзей – ня толькі ўдзельнікі супраціву і палітычныя дзеячы, але і бізнэсоўцы, і праграмайстры, і проста людзі, якія ня хочуць, каб дзяржава совала свой мандат у непатрэбныя рэчы. Так што ў гэтым натоўпе даволі проста схавацца.

Калі вы карыстаецеся Unix-падобнымі сыстэмамі, стварэньне ВШД ня будзе праблемай, дапрыкладу, можаце выкарыстоўваць EncFS у Linux, а ў FreeBSD існуе зручны і надзейны **gbde**. Калі вы аднолькава часта карыстаецеся Windows і якім кольвек юніксам на адной машыне, для вас ёсьць сэнс зірнуць у бок **BestCrypt for Linux**, ды сачыце таксама за праектам **TrueCrypt** – ён будзе партаваны ў Linux бліжэйшым часам - зможаце карыстацца адным і тым жа сродкам у розных сыстэмах.

Для шыфроўкі асобных файлаў падыдуць **PGP** і **GPG**, даступныя для самых розных апэрацыйных сыстэмаў. Абедзьве праграмы маюць добрую рэпутацыю і пры гэтым сумяшчальныя міжсобку.

Дзе ўзяць

Выладоўвайце TrueCrypt з сайту **truecrypt.sourceforge.net**, **PGP**, у тым ліку **PGPdisk** – з **pgpi.com**, а на **gpg.org** адпаведна атрымаеце **GPG**. Што датычыцца **BestCrypt**, то гэтая праграма даступная на сайце вытворцы: **jetico.fi**, зьвярніце, аднак, увагу, што вэрсія для Windows спыніць сваю працу праз 30 дзён (праграма ўмоўна бясплатная).

У любым выпадку, засьцерагайцеся набываць крыптаграфічныя сродкі на кампутаровых рынках – там вам могуць уперці дзіравую вэрсію, якая ня будзе надзейным сродкам шыфраваньня (кепска, што самі вы гэтага адразу не заўважыце).

Рэзэрвовая копія

Калі ваш кампутар (ваш дыск, іншы носьбіт інфармацыі) будзе скрадзены альбо канфіскаваны, ліхадзеі альбо «праваахоўнікі» будуць мець вашыя файлы, калі вы ігнаравалі патрабаваньні бясьпекі, і ня будуць нічога мець, калі інфармацыя надзейна зашыфраваная. Аднак глянем на сытуацыю зь іншага боку – вы таксама ня будзеце мець вашых файлаў! Нечакана (а такія рэчы заўсёды адбываюцца нечакана) апынуцца без дакумэнтаў, архіваў, базаў зьвестак, перапіскі, сьпісу кантактаў, уласных плянаў і напрацовак – гэта амаль заўсёды азначае паралюш арганізацыі і страты, часьцяком незваротныя.

Каб спаць спакойна, трэба ня толькі пазбавіць ня вартых даверу людзей доступу да інфармацыі, але й забясьпечыць надзейны доступ для сябе ў экстраардынарных сытуацыях. Для гэтага абавязкова трэба рабіць **пэрыядычныя рэзэрвовыя копіі** ўсіх важных зьвестак (зразумела, таксама ў зашыфраваным варыянце) – напрыклад, раз на паўгоду рабіць рэзэрвовую копію ўсяго таго, што было напрацавана арганізацыяй.

Важна! Сакрэтная інфармацыя запісваецца на рэзэрвовы носьбіт-копію толькі ў зашыфраваным выглядзе! Калі вы карыстаецеся віртуальнымі шыфраванымі дыскамі – найпрасьцей капіяваць увесь файл, які ўтрымлівае дыск. Адсюль вынікае яшчэ адна парада – ствараючы ВШД, вызначайце яго памер ня большым за ёмістасьць носьбіта, на які вы звычайна робіце копію. Заўсёды правярайце, ці запісалася копія без памылак. Праграмы, што запісваюць CD і DVD, звычайна маюць опцыю «праверыць запіс» (анг. verify), – абавязкова ўключыце яе.

Спосабы рабіць рэзэрвовыя копіі

Найпрасьцейшы варыянт зрабіць рэзэрвовую копію – запісаць файлы на **CD**. Для гэтага ваш кампутар мусіць быць аснаджаны CD-recorder'ам (гэтая прылада выглядае як звычайны CD-rom, але дазваляе ня толькі чытаць, але й запісваць дыскі). Запіс вядзецца на пустыя дыскі-»матрыцы» (званыя таксама «балванкамі»). Матрыцы бываюць двух тыпаў: CD-R, які запісваецца аднойчы і назаўсёды, і CD-RW, які можна перазапісваць некалькі разоў. Стандартная ёмістасьць – 700 Mb. Запіс звычайна не падобны да простага капіяваньня файлаў, бо неабходна адмысловая праграма для запісу. Карыстальнікі Windows XP ды Unix-падобных сыстэмаў маюць такія магчымасьці, іншым можна ўсталяваць Nero Burning Rom.

Калі інфармацыі надта многа, спатрэбіцца многа «балванак» і шмат часу, каб іх запісваць. У такім разе найлепшым варыянтам можа стаць запіс на матрыцы **DVD**, ёмістасьць якіх значна большая. Вам спатрэбіцца DVD-recorder. Улічыце, што далёка не на кожным кампутары можна чытаць DVD – CD-ROM'ы ўсё-ткі сустракаюцца часьцей.

Запіс на модулі **флэш-памяці** («флэшкі») цяпер робіцца папулярным сродкам захоўваньня і транспартаваньня каштоўнай інфармацыі. Плюсам гэтага мэтаду зьяўляецца тое, што «флэшка» часьцяком не выглядае як носьбіт інфармацыі – звычайна гэтыя модулі выглядаюць як бралок, запальніца, падвесак, кулон ці кароткі флямастэр. Модулі флэш-памяці ўстаўляюцца ў порт (разьём) USB (чытаецца Ю-Эс-Бі). Для Windows 98/95 спатрэбяцца праграмы-драйвэры, зазвычай яны даступныя ў Інтэрнэце, бальшыня астатніх сыстэмаў адчыняе іх аўтаматычна. Запіс адбываецца простым капіяваньнем файлаў. Многія любяць «флэшкі» за малы памер і зручнасьць выкарыстаньня. Аднак, на наш погляд, «флэшкі» хутчэй падыходзяць для транспартаваньня канфідэнцыйнай інфармацыі – але гэта кепскі варыянт, калі вядзецца пра рэзэрвовае капіяваньне, паколькі яны недастаткова надзейныя і зьмяшчаюць адносна нямнога інфармацыі (найбольш пашыраныя варыянты 128, 256 і 512Mb). Флэш-модулі часам прадугледжваюць доступ з паролем, але, як і ў выпадку паролю да кампутара альбо незашыфраванага файлу, не спадзявайцеся на яго: мэтафарычна кажучы, гэта ня сэйф, а драўляная шуфлядка. З «флэшкамі» гэтаксама трэба быць пільнымі і асьцярожна выкарыстоўваць іх у якасьці адзінага (асноўнага) носьбіту інфармацыі – менавіта дзеля сваёй кампактнасьці і непрыкметнасьці яны могуць лёгка згубіцца ці іх могуць скрасьці.

Яшчэ адзін падобны сродак захоўвання рэзэрвовых копіяў – **мр3-плэеры, смартфоны і іншыя побытавыя прылады зь вялікім аб'ёмам памяці**. Яны выкарыстоўваюцца як флэшкі, але ў пэўных сытуацыях выклікаюць менш падазрэньняў.

Параўнальная табліца ўласьцівасьцяў рэзэрвовых носьбітаў інфармацыі

Носьбіт	Надзейнасьць	Тэрмін прыдатнасьці	Зручнасьць	Ёмістасьць
CD	Адносна высокая	Залежыць ад маркі матрыцы і частаты выкарыстаньня. Аднойчы запісаны дыск можа праляжаць "бяз руху" ня менш за 3 гады. Інтэнсіўнае чытаньне істотна зьмяншае гэты тэрмін	Вымагае пэўнай падрыхтоўчай працы і выкарыстаньня адмысловага праграмнага забесьпячэньня	700 Mb
DVD	Гл. папярэдні п.	Гл. папярэдні п.	Гл. папярэдні п.	Залежыць ад фармату, часьцей 4,7 Gb
Флэш-модуль	Нізкая	Моцна залежыць ад маркі, але ў кожным разе вельмі няпэўны. Часам псуецца праз тыдзень, часам працуе колькі год.	Зручна. Бачны ў сыстэме як дыск альбо каталёг. Адпаведна можна рабіць усе стандартныя апэрацыі – чытаць, пісаць, зьмяняць – звычнымі сродкамі. Непрыкметны для неабазнанага вока.	Найчасьцей сустракаюцца мадэлі 128 Mb, 256 Mb, 512 Mb
Вонкавы дыск	Адносна высокая. Але такія прылады часьцяком адчувальныя да ўдараў і вымагаюць асьцярожнасьці	Пры акуратным карыстаньні можна разьлічваць прынамсі гадоў на 5.	Зручна. Таксама як і ў папярэднім п.	Разнастайныя, але ж ня менш за колькі гігабайт

Запіс на **вонкавыя дыскі** таксама зьяўляецца добрым варыянтам для вырабу рэзэрвовых копіяў. Працаваць зь імі зручна, а аб'ём запісанай інфармацыі – вялікі. Вонкавы дыск – па-сутнасьці звычайны «цьвёрды» дыск, накшталт таго, што знаходзіцца ўнутры вашага кампутара, але вынесены ў асобны корпус. Ён падключаецца да кампутара кабэлем праз порт USB альбо COM-порт.

У якасьці рэзэрвовай копіі (нагадаем – для зашыфраванай інфармацыі) можна выкарыстоўваць **бясплатны хостынг і паштовыя скрыні** ў Інтэрнэце. Падобную паслугу робіць *gmail.com* (памер – 2 гігабайта) і шмат іншых рэсурсаў (некаторыя зь іх дазваляюць карыстацца аўтаматычным шыфраваньнем пры перадачы дадзеных з вашага кампутара – паводле аналёгіі з кіраваньнем банкаўскім рахункам праз Інтэрнэт). Гэты від захоўваньня цяпер набывае папулярнасьць ува ўсім сьвеце, паколькі зь любога месца можна дабрацца да сваёй інфармацыі і нават можна выкарыстоўваць яе як хард-дыск для вашага ноўтбука ці іншага гасьцявога кампутара. Аднак пакуль у Беларусі гэты сродак не распаўсюджаны з прычыны невялікай хуткасьці сувязі.

Захаваньне рэзэрвовых копіяў

Няма нічога дурнейшага, як зрабіць рэзэрвовую копію і пакінуць яе каля кампутара – у гэтым папросту няма ніякага сэнсу, менты альбо рабаўнікі ў выпадку форс-мажору атрымаюць і асноўную, і рэзэрвовую копію. Выснова: копіі трэба перахоўваць у іншым памяшканьні. Ці можна папросту забраць іх дахаты? У прынцыпе, мы ня ведаем – пакуль – выпадкаў, калі б вобшукі ці крадзяжы праводзіліся адначасова ў офісах і прыватным жытле актывістаў. Аднак такое можа адбыцца заўтра – гэта ўваходзіць у лемантар «праваахоўнай» дзейнасьці спэслужбаў. Ня варта захоўваць рэзэрвовую копію ў офісе іншай няўрадавай арганізацыі ў вашым горадзе – выпадкі правядзеньня некалькіх адначасовых вобшукаў у офісах некалькіх арганізацыяў ужо былі зафіксаваныя. З тых жа прычынаў ня варта захоўваць рэзэрвовыя копіі ў офісах арганізацыяў, якія ўваходзяць у адну сетку. Найлепшы варыянт – аддаць іх надзейнаму чалавеку, які не працуе ў вашым офісе стала, альбо захаваць іх у надзейнага сябра. Можаце рабіць некалькі копіяў адначасова і захоўваць іх у розных месцах – гэта павялічвае абсяг працы, але імавернасьць поўнага зьнікненьня інфармацыі ў такім разе блізкая да нулю.

Каб вырашыць, ці трэба вам гэта, уявіце сябе ў сытуацыі, калі вашая інфармацыя зьнікла, – наколькі гэта страшна менавіта для вас?

Як карыстацца электроннай поштай?

Інфармацыю зручна перасылаць праз электронную пошту, аднак вашыя лісты лёгка могуць быць перахопленыя. Для таго каб захоўваць бясьпеку, вам трэба карыстацца **PGP** альбо **GPG** – абедзьве праграмы ўзаемазамяняльныя, аднак для карыстальнікаў Windows лепш падыдзе першая. Абменьвайцеся з вашымі карэспандэнтамі ключамі, шыфруйце файлы, якія перасылаеце, і пачувайце сябе бясьпечна – ніхто вашую перапіску напэўна не прачытае. Але пры гэтым захоўваецца небясьпека, што «ворагі» будуць ведаць, паміж якімі з «падазроных» паштовых скрыняў ідзе актыўная перапіска з выкарыстаньнем **PGP** альбо **GPG,** – часам гэта зьяўляецца непажаданым (напрыклад калі вы перапісваецеся зь нейкім вядомым замежным карэспандэнтам). У мэтах прадухіленьня гэткай небясьпекі варта завесьці для асабліва канфідэнцыйнай перапіскі адмысловыя паштовыя скрыні. Калі вам трэба пераслаць асабліва канфідэнцыйную інфармацыю – вядома, зашыфраваную, – варта стварыць выключна дзеля гэтага выпадку спэцыяльную паштовую скрыню, якой вы скарыстаецеся толькі адзін раз з калектыўнага» выхаду ў Інтэрнэт (напрыклад, з інтэрнэт-кавярні).

Таксама пры карыстаньні электроннай поштай варта карыстацца самымі простымі правіламі асьцярожнасьці – націскаць «выхад» («sign out» альбо «log out») перад тым, як зачыніць старонку з поштай, выкарыстоўваць найбольш бясьпечныя зь існых на вашым сэрвэры варыянтаў падлучэньня (напрыклад, для карыстальнікаў паштовага сэрвісу Yahoo! прапануецца два віды падлучэньня – стандартны і бясьпечны (secure) – мэтазгодна карыстацца апошнім), пэрыядычна мяняць паролі, не карыстацца простымі паролямі, не паведамляць пароль праз тэлефон і не казаць іншым людзям. Натуральна, вельмі небясьпечна карыстацца паштовымі сэрвісамі, што даступныя для беларускіх спэцслужбаў, напрыклад tut.by, а таксама ня варта перасылаць на тутбаеўскія скрыні канфідэнцыйную інфармацыю. Існуюць таксама паштовыя сэрвэры, якія маюць убудаваную сыстэму шыфраваньня, адзін з найбольш вядомых – hushmail.com. Не было б нічога дзіўнага, калі б высьветлілася, што за гэтымі сэрвэрамі стаяць спэцслужбы ЗША ці Брытаніі, аднак для нас гэта вялікай ролі ня грае: абы не гэб'ё.

У працы з электроннай поштай існуе некалькі простых і надзвычай важных правілаў: ніколі не карыстайцеся праграмамі Outlook альбо Outlook Express ад фірмы Microsoft; ніколі не адчыняйце дадаткаў (attachments) няяснага альбо (нібыта) забаўляльнага прызначэньня, у тым ліку мульцікаў, праграмаў ды архіваў, пароль да якіх прапануецца ў целе ліста.

Пытаньні выкарыстаньня PGP

*Чаму неабходна карыстацца **PGP**?* З тых самых прычын, зь якіх вы заклейваеце ліст у капэрту альбо не дазваляеце чытаць цераз вашае плячо. Стандартныя сродкі электроннай пошты не забясьпечваюць аніякай канфідэнцыйнасьці вашаму ліставаньню. Перад тым як дайсьці да адрасата, вашае паведамленьне пройдзе празь некалькі кампутараў менавіта ў тым выглядзе, у якім вы яго стварылі, – г. зн. адкрыты тэкст і даступныя дадаткі (attachments). На кожным этапе паведамленьне можа быць прачытанае. Ясна, што ў варунках дыктатуры гэта набывае асаблівае значэньне, бо ўладныя структуры ад КДБ і да чыноўнікаў сярэдняга гатунку могуць лёгка і часта карыстацца гэтай магчымасьцю. Дадайце да гэтага, што адміністратарамі тых кампутараў і сетак, празь якія вы адсылаеце, пошту могуць быць людзі занадта цікаўныя і недастаткова сумленныя і, магчыма, яны чуйныя да «настойлівых просьбаў» з боку гэбэшнікаў .

Ці існуюць іншыя падобныя праграмы? Так, існуюць. Але **PGP** – найбольш аўтарытэтны і найшырэй распаўсюджаны прадукт на гэтым рынку. Ён разьлічаны на карыстальніка сярэдняй кваліфікацыі, вымагае некаторага навучаньня, але працаваць зь ім прасьцей, чым зь якімкольвек Word'ам. Дазваляе шыфраваць кавалкі тэксту і файлы любых фарматаў. Мае бясплатную вэрсію. На цяперашні час **PGP** – сусьветны стандарт для офіснай бясьпекі.

*Наколькі надзейны **PGP**? «У сьвеце ёсьць два гатункі крыптаграфіі: адзін ня дасьць тваёй малодшай сястры чытаць твае файлы, другі ня дасьць моцным урадам чытаць твае файлы»* (Bruce Schneier, Applied Cryptography). Апошні варыянт называецца моцнай крыптаграфіяй. PGP належыць да клясы моцных крыптаграфічных праграм. Калі вы карыстаецеся PGP у адпаведнасьці з рэкамэндацыямі распрацоўніка, вашае паведамленьне наўрад ці будзе расшыфраванае. Беручы ў якасьці прыкладу здольнасьці сучасных кампутараў, для расшыфроўкі правільна зашыфраванага паведамленьня аднаму мільяр-

ду кампутараў спатрэбіцца больш часу, чым праіснуе Сонечная сыстэма. Уражвае?

Зразумела, кампутарная тэхніка ўвесь час прагрэсуе і праз нейкі час можа адбыцца тэхналягічны прарыў, які зробіць расшыфроўку больш магчымай. Але, арыентуючыся нават на самыя сьмелыя прагнозы, у вас у запасе дзесяцігодзьдзі. Хто стане працаваць так доўга дзеля вашай перапіскі? Часьцяком можна пачуць: «Я прачытаў у Інтэрнэце, што КДБ умее расшыфроўваць PGP» ці штосьці гэткага ж фармату. Фокус у тым, што спэцслужбы зацікаўленыя ў дыскрэдытацыі PGP ды іншых крыптасыстэм менавіта таму, што яны ня могуць яе адужаць! Адсюль падобныя выкіды дэзінфармацыі. Спэцслужбы таталітарных рэжымаў схільныя да парушэньня законаў, але законы матэматыкі – хрэн парушыш!

Ці ня можа так быць, што распрацавальнікі праграмы зрабілі схаваную «дзірку» ў кодзе праграмы і робяць падвойны бізнэс, прадаючы людзям крыптасыстэму, а ўрадам – магчымасьць яе ўзламаць? Зь іншай праграмай гэта магчыма, але распрацавальнікі PGP прытрымліваюцца палітыкі «адкрытага коду». Гэта значыць, што кожны, хто пажадае, можа атрымаць праграму ў «сырым» выглядзе і прааналізаваць яе. Тысячы незалежных праграмістаў ужо зрабілі гэта, і тысячы робяць гэта цяпер. Гэта ня толькі гарантуе адсутнасьць злых сюрпрызаў, але і дазваляе вылоўліваць магчымыя памылкі.

Важная заўвага: для таго каб пададзенае тут было праўдай, вашая **PGP** павінна быць *вартай даверу*, скачанай з www.pgpi.com.

Як працаваць з PGP?

Стварэньне пары ключоў

Стварэньне новай пары ключоў адбываецца ў двух выпадках: калі вы ўпершыню ўсталёўваеце PGP – тады праграма сама прапануе пачаць працэс стварэньня – альбо вам проста спатрэбілася згенэраваць новую пару. У апошнім варыянце вам трэба ў мэню *Keys* выбраць *New key*.

1. Увядзіце сваё імя ў поле *Full name* і паштовы адрас (электроннай пошты, зразумела) – у поле *Email address*. Гэтыя зьвесткі будзе бачыць той чалавек, якому вы дасьцё свой адкрыты ключ. Вы можаце, калі вам захочацца, пазначыць тут мянушку альбо псэўданім ды й адрас фальшывы… Толькі калі гэта заблытае вашых карэспандэнтаў – ня скардзіцеся.

2. У акенца *Passphrase* уводзьце фразу-пароль. Так, так, ня слова, а

фразу! Паводле таго, як вы ўводзіце пароль, сыстэма ацэньвае яго якасьць у полі *Passphrase quality.* Па змаўчаньні ЗПЗ не паказвае тое, што вы набіраеце, – раптам хтосьці падглядае? Але калі ніхто не падглядае, можаце зьняць гачок з опцыі *Hide typing* – набіраць стане прасьцей.

У акенца *Confirm* трэба зноўку ўвесьці пароль. Гэта можа падацца дзіўным, але ўвод паролю – надзвычай адказны момант і падвойная праверка дазволіць зьменшыць імавернасьць абдрукоўкі.

3. Праграма генэруе пару ключоў: сакрэтны і адкрыты. Проста чакайце, працэс можа заняць некалькі хвілінаў.

Захоўванье і чытаньне ключоў

Запусьціце PGPKeys. Выберыце ваш ключ, ідзіце ў мэню *Keys,* націсьніце каманду *Export.* Вам прапануецца выбраць месца ды назву файлу, у якім будзе захаваны ключ. Працэдура такая ж, як пры захаваньні дакумэнту Word. Ёсьць важная акалічнасьць – опцыя *Include private key(s).* Па змаўчаньні яна выключаная – і гэта значыць, што будзе захаваны толькі адкрыты ключ. Вы можаце разаслаць яго сваім рэцыпіентам. Калі вы паставіце гачок для гэтай опцыі, будзе захаваная пара ключоў (і сакрэтны, і адкрыты). Дасылаць пару ключоў, вядома, нікому нельга. Пару захоўваюць толькі каб зрабіць копію (напрыклад, каб перанесьці на новы кампутар альбо проста захаваць копію ў надзейным месцы).

Для чытаньня ключоў выканайце каманду *Import* у мэню *Keys* ды знайдзіце файл, што ўтрымлівае ключ(ы). Праграма пакажа, якія ключы захоўваюцца ў гэтым файле, – іх можа быць некалькі. Выберыце патрэбныя і націсьніце *Import.*

Спраўджваем адбіткі

У акне PGPKeys выберыце патрэбны ключ, кляцніце правую кнопку мышкі, выберыце пункт *Key properties* – убачыце сьпіс словаў у рамцы з загалоўкам *Fingerprint* – гэта і ёсьць адбітак. Перапішыце яго, каб спраўдзіць у тэлефоннай размове альбо падчас асабістай сустрэчы.

Шыфруем файл

1. У любой праграме Windows, якая прадугледжвае працу з файламі, вылучаем адзін ці некалькі файлаў і кляцаем правай кнопкай мышкі. Зьявіцца мэню з шэрагам пунктаў, сярод іх выбераце PGP – адкрыецца

падмэню. Каманда *Encrypt* шыфруе файлы, *Encrypt & Sign* – шыфруе і падпісвае. Выберыце неабходны вам варыянт.

2. Адчыніцца акно: уверсе – сьпіс адкрытых ключоў, якія ўсталяваныя ў вашым кампутары, ніжэй – пустое поле. У яго вам трэба перацягнуць мышкай ключы тых людзей, для якіх вы шыфруеце вашыя файлы (вашых рэцыпіентаў). Вы можаце шыфраваць і для сябе, для гэтага перацягніце свой ключ.

Кожны з тых, чые ключы будуць перанесеныя ў поле *Recipients*, зможа расшыфраваць файлы сваім сакрэтным ключом незалежна ад іншых рэцыпіентаў.

З паказаных унізе опцыяў мы прапануем вашай увазе толькі адну – *Wipe original*. Калі яна выключаная, у выніку шыфраваньня будуць створаныя шыфраваныя вэрсіі выбраных файлаў, але арыгіналы застануцца некранутымі. Уключыўшы ж яе, вы загадаеце праграме зьнішчыць арыгіналы (застануцца толькі зашыфраваныя вэрсіі). Зьнішчэньне адбудзецца такім чынам, што ўзнавіць файлы ня ўдасца.

3. Калі вы выбралі каманду *Encrypt & Sign*, вам будзе прапанавана выбраць ключ, якім вы хочаце падпісаць файлы, ды ўвесьці пароль.

Шыфруем кавалак тэксту

Тыповая задача: вы напісалі ліст і вырашылі адправіць яго ў зашыфраваным выглядзе. Вылучаем тэкст, капіюем яго ў «кішэнь» сыстэмы.

Кляцаем правай кнопкай мышкі на памянёным ужо замочку каля гадзіньніка. Выбіраем каманду *Clipboard*, потым – *Encrypt* альбо *Encrypt & Sign*, калі вы хочаце яшчэ і падпісаць тэкст.

Далей праца такая ж, як падчас шыфраваньня файлаў. Па завяршэньні ў сыстэмнай «кішэні» будзе знаходзіцца зашыфраваны кавалак. Устаўце яго ў патрэбную праграму (напрыклад у паштавік).

Расшыфроўка файлаў

У бальшыні выпадкаў дастаткова двойчы кляцнуць мышкай па зашыфраваным файле. Праграма запытае пароль і расшыфруе.

Расшыфроўка тэксту

Скапіюйце зашыфраваны тэкст ад радка з пазнакай «BEGIN PGP MESSAGE» да радка «END PGP MESSAGE» улучна. Праз замочак выклічце мэню *Clipboard*, потым – *Decrypt & Verify*.

Расшыфраваная інфармацыя ў «кішэні».

Даведнік тэрміналёгіі PGP

Ключ *(key)* – гэта зьвесткі, неабходныя для зашыфроўкі ці расшыфроўкі інфармацыі. Захоўваюцца ў файлах.

Памер ключа *(key size)* – памер таго пакету зьвестак, які зьяўляецца ключом. Чым большая даўжыня ключа, тым больш часу і высілкаў неабходна зламысьніку, каб яго падабраць. Вымяраецца ў бітах.

Адкрыты (ці публічны) **ключ** *(public key)* – ключ, якім можна толькі зашыфроўваць інфармацыю. Вы павінны распаўсюдзіць гэты ключ сярод тых, хто будзе пісаць вам шыфраваныя лісты.

Сакрэтны (ці прыватны ключ) **ключ** *(private key)* – ім можна расшыфроўваць інфармацыю, зашыфраваную адкрытым ключом. Сакрэтны ключ – толькі для вас, ахоўваце яго ад пабочных асобаў. На выпадак, калі яго ўсё-ткі скрадуць, сыстэма PGP прадугледжвае пароль, ня ведаючы якога, сакрэтным ключом не скарыстаешся.

Адбітак ключа *(key fingerprint)* – даволі доўгі набор ангельскіх словаў, унікальны для кожнага ключа. Рэч у тым, што адкрыты ключ, які вам даслаў ваш сябра, неабавязкова дайшоў. Яго можна падмяніць, каб потым чытаць вашую карэспандэнцыю. Таму ключы трэба зьвяраць праз тэлефон ці на асабістай сустрэчы, параўноўваючы іх адбіткі. Калі ўсе словы супадаюць –значыцца, ключ той; калі не супадаюць – ключ падмянілі.

Пара ключоў *(key pair)* – у PGP ключы ствараюцца толькі парамі: сакрэтны + адкрыты. Вы лёгка зразумееце чаму – калі ўважліва прачыталі, чым адрозьніваюцца сакрэтны й адкрыты ключы.

Рэцыпіент *(recipient)* – кажучы папросту, тая асоба, для якой вы шыфруеце інфармацыю, атрымальнік, адрасат. Каб зашыфраваць штосьці для пэўнага рэцыпіента, вы мусіце мець ягоны адкрыты ключ. Перачытайце пункт «Адкрыты ключ», калі не разумееце чаму.

Ліставаньне – у кантэксьце PGP – абмен шыфраванымі паведамленьнямі ці файламі. Каб ліставаньне паміж вамі і іншым чалавекам было магчымае, вы мусіце абмяняцца сваімі адкрытымі ключамі (гл. папярэдні пункт).

Подпіс *(digital signature)* – грае тую ж ролю, што і звычайны рукапісны подпіс: засьведчвае тэкст і любы іншы тып зьвестак, што дазваляе ў далейшым спраўдзіць ці высьветліць паходжаньне інфармацыі.

Подпіс у PGP робіцца сакрэтным ключом, наколькі дзіўна гэта б ні гучала для непадрыхтаванага вуха. Электронны подпіс можа спадарожнічаць шыфроўцы (інфармацыя, зашыфраваная адкрытым клю-

чом рэцыпіента і падпісаная вашым сакрэтным ключом) альбо проста засьведчваць незашыфраваныя зьвесткі. Можа захоўвацца ў асобным файле альбо ў адным з падпісанай інфармацыяй.

PGPTools, PGPKeys – часткі праграмы PGP. Любую зь іх можна запусьціць праз мэню *Пуск (Start)* альбо кляцнуўшы правай кнопкай мышкі на замочак, які PGP, па ўсталяваньні, разьмяшчае каля гадзіньніка, у правым ніжнім куце экрану.

Лякальная кампутаровая сетка і праца ў Інтэрнэце, вірусы і траяны

Падключэньне да Інтэрнэту вашага кампутара дае ворагам неблагія шанцы для выкраданьня інфармацыі. Па-першае, у вас можа быць незаўважна ўсталяваная праграма-шпег, закінутая вам у выглядзе вірусу ці траяну і, ледзь толькі вы ўвойдзеце ў Сусьветнае павуціньне, яна пачне перасылаць інфармацыю з вашага дыска зламысьнікам. Падругое, сама апэрацыйная сыстэма можа мець «дзіркі» і памылкі, якія даюць магчымасьць нягоднікам кіраваць вашым кампутарам праз Інтэрнэт (асабліва гэтым «славіцца» Windows, якая найбольш распаўсюджаная ў нашай краіне).

Такім чынам, карыстаньне Інтэрнэтам дапушчальнае толькі ў тым выпадку, калі вы ўсталюеце сабе праграму-фаервол (анг. firewall) ды антывірус. Фаервол – гэта праграмны сродак, які блякуе недазволеныя сеткавыя апэрацыі, перашкаджаючы шкодным праграмам высылаць штосьці ў Інтэрнэт і зачыняючы доступ да вашага кампутара звонку (з Інтэрнэту). Для карыстальнікаў Windows можна парэкамэндаваць Norton Internet Security, які да таго ж можна ўсталяваць у пары з Norton Antivirus. Людзі ж, якія працуюць з Unix-падобнымі апэрацыйнымі сыстэмамі, збольшага ўратаваныя ад праблемаў зь вірусамі, а фаервол маюць адпачатку (магчыма, яго трэба ўключыць). У Windows XP таксама ёсьць убудаваны фаервол (брандмаўэр), аднак многія людзі не давяраюць ягонай надзейнасьці.

Трэба зазначыць, што абарончае праграмнае забесьпячэньне вымагае настройкі, і вам неабходна будзе паглыбіцца ў вывучэньне суправаджальнай дакумэнтацыі альбо скарыстаць з паслугаў чалавека, якому вы *давяраеце*.

У выпадку зь лякальнай сеткай лічыцца больш надзейным на той кампутар, які непасрэдна падлучаны да Інтэрнэту, ускласьці абавязкі **выключна** фаерволу і шлюза (разьмеркавальніка Інтэрнэту для

іншых кампутараў сеткі) і не працаваць на ім з канфідэнцыйнай інфармацыяй.

Калі ў вашай лякальнай сетцы працуюць людзі, якія не ўваходзяць у *кола даверу*, пажадана не адкрываць сеткавы доступ да тых дыскаў і каталёгаў, што зьмяшчаюць сакрэтную інфармацыю, альбо прынамсі абараняць іх паролем.

Павінна існаваць пісьмова афармленая палітыка бясьпекі ў дачыненьні да кампутараў і сеткі. Усталяваньнем і настройкай праграмаў павінен займацца толькі адзін адказны чалавек – адміністратар сеткі. Ён абавязаны прытрымлівацца праактыўнага падыходу да патэнцыйных праблемаў: павышаць сваю кваліфікацыю, чытаць электронныя бюлетэні, прысьвечаныя праблемам бясьпекі, рэгулярна абнаўляць апэрацыйную сыстэму, антывірус ды іншыя абарончыя праграмы. Трэба рэгулярна ставіць «заплаткі» на праблемныя месцы ў апэрацыйнай сыстэме і праграмах, што працуюць з Інтэрнэтам.

Прагляднік Internet Explorer, усталяваны па змаўчаньні на кожным кампутары з Windows, мае вельмі дрэнную рэпутацыю: цягам доўгага часу ў ім знаходзілі ўсё новыя і новыя дзіркі, якія даюць ліхадзеям магчымасьці для пранікненьня ў ваш кампутар. Пазьбягайце гэтай праграмы! Усталюйце лепш Mozilla Suite ці Mozilla Firefox, што даступныя бясплатна.

Якія існуюць небясьпекі ў захоўваньні кампутаровай інфармацыі?

Небясьпекі ў захоўваньні і перадачы інфармацыі абумоўленыя працоўнымі сытуацыямі. Бясьпека вашай інфармацыі залежыць ад вашага абсталяваньня, вашага праграмнага забесьпячэньня, апэрацыйнай сыстэмы, вашых паводзінаў і парадку ў вашым офісе.

Энэргазахаваньне – таксама праблема бясьпекі. Бальшыня сучасных кампутараў аснаджаныя сыстэмай энэргазахаваньня, якая выключае часткі абсталяваньня, калі пэўны час ніхто не працуе з кампутарам. Пры гэтым зьмесьціва памяці можа быць скінутае на дыск – а ў памяці могуць знаходзіцца дакумэнты, зь якімі вы працуеце. Зламысьнік можа прасканаваць ваш дыск у пошуку «адбітку памяці», і ёсьць імавернасьць, што яму пашанцуе. Адключыце энэргазахаваньне ў настройках вашай сыстэмы! Зьвярніце ўвагу на тое, што для ноўтбукаў адключэньне можа быць немагчымым альбо можа прывесьці да хуткай разрадкі акумулятараў.

Апэрацыйная сыстэма пэрыядычна скідае кавалкі памяці на дыск у г. зв. «файл падкачкі», каб вызваліць месца для пэўных патрэбаў. Адпаведна ўзьнікае тая ж небясьпека, што і ў папярэднім пункце, аднак, на шчасьце, у меншым маштабе. Адключыць гэтую функцыю, не рызыкуючы стабільнасьцю сыстэмы, немагчыма. У некаторых выпадках можна аўтаматычна шыфраваць файл падкачкі. Карыстальнікі Unix-падобных сыстэмаў маюць такую магчымасьць у самой сыстэме, для Windows XP можна выкарыстаць BestCrypt v.7, аднак гэтая праграма каштуе грошай. Для Windows 98/95 праблема невырашальная.

Ноўтбук – фактар рызыкі. Апроч апісанай вышэй праблемы з энэргазахаваньнем, пераносныя кампутары лягчэй скрасьці, у стомленым стане вы можаце і проста пакінуць яго недзе. Дадамо, што ноўтбук можа быць сканфіскаваны падчас дагляду аўтамабіля ці асабістых рэчаў альбо падчас праезду праз мяжу. Не захоўвайце ў сваім «мабільным офісе» вялікіх масіваў канфідэнцыйнай інфармацыі, захоўвайце толькі тыя рэчы, зь якімі вы зьбіраецеся працаваць бліжэйшым часам. Зразумела, усё павінна быць зашыфраванае.

Небясьпекі выдаленых файлаў. Проста выдаліць файл – менш за паўсправы. Сыстэма проста пазначае «месца, занятае гэтым файлам, лічыць свабодным», але нічога не вынішчае. Адмысловымі сродкамі можна аднавіць файл альбо яго часткі і прачытаць. Замест таго каб выдаляць (анг. delete), файлы трэба вынішчаць (анг. wipe)! Для гэтага выкарыстоўваюцца праграмныя сродкі, прадугледжаныя, напрыклад, у **PGP** (націскаеце правай кнопкай мышкі на файл, выбіраеце **PGP,** выбіраеце wipe – і ваш файл выдаляецца надзейна).

Парадак доступу да кампутараў. Чужы чалавек за кампутарам – катастрафічна небясьпечна! Ён можа занесьці вірус альбо выпадкова прачытаць важную інфармацыю, ён можа аказацца аматарам парнаграфіі (і файлы, якія ён пакіне па сябе, скампрамэтуюць вас). І гэта толькі ў тым выпадку, калі ён не зламысьнік. Калі ж ён мае на мэце шпігоўства – ён можа ўнятрыць у ваш кампутар праграмы, якія перахопяць вашыя паролі і зьвядуць на нуль усю вашую бясьпеку. Дасьведчаны чалавек можа гэта зрабіць нават калі за ім назіраюць.

Неабходна распрацаваць (пажадана ў пісьмовым выглядзе) парадак доступу да кампутараў. Калі для вас неабходна пускаць іншых людзей папрацаваць на вашыя кампутары, вылучыце адну-дзьве машыны, на якіх будзе адбывацца праца з закрытымі дакумэнтамі, і абмяжуйце да іх доступ.

Асаблівую асьцярожнасьць трэба мець з выкарыстаньнем дыскетаў, звычайна на іх «забываецца» інфармацыя, якая ў працэсе працы была прынесеная ў офіс звонку. Пажадана, каб у офісе не валяліся ўжываныя дыскеты «пра запас».

Узломнікі сыстэмаў карыстаюцца ня толькі тэхнічнымі сродкамі, але і актыўным сацыяльным інжынэрынгам. Вельмі проста – патэлефанаваць і ад чужога імя спытаць нібыта забыты пароль. Часта спрацоўвае. Чытайце біяграфію Кевіна Мітніка, самага «раскручанага» ўзломніка сыстэмаў.

Гіпэртрафія ветлівасьці – крыніца правалаў. Сярэдні беларус, як той японец, ня ўмее казаць цьвёрдага «не». Прыходзіць, дапрыкладу, у арганізацыю невядомы з чыстым позіркам і, гледзячы проста ў вочы, задае нясьціплыя пытаньні, альбо просіць «на хвілінку» пусьціць да кампутара, альбо імпэтна прапануе свае паслугі ў якасьці добраахвотніка. Выглядае прыстойна, імкнецца гаварыць па-беларуску, на свае паводзіны мае тлумачэньні. Ай, як жа адмовіць, няветліва ж! Проста дзіва бярэ, як часта гэты – просты ў прынцыпе – фокус спрацоўвае і людзі сваімі рукамі здаюць канфідэнцыйную інфармацыю.

Іншы варыянт – нахабства. Вы чытаеце важную паперыну ці зьбіраецеся ўвесьці пароль на сваім кампутары, а гэтым часам цераз вашае плячо, не хаваючыся, пачынае пазіраць іншы чалавек. У такой сытуацыі многія людзі няздольныя даць адпор нахабніку і ў выніку «паляць» інфармацыю.

Пераадолець злачынную ветлівасьць дапаможа невялікая доза бюракратыі. Распрацоўвайце правілы, што можна, а чаго нельга. Каму можна сядаць за гэты кампутар, а каму – за гэны. Доступ да дакумэнтаў трэба даваць толькі тым людзям, якія зь імі працуюць. Вызначце, які стаж павінен напрацаваць у вашай арганізацыі чалавек, якія тэсты прайсьці, каб атрымаць свой статус у вашым офісе. Усе правілы павінны быць разьмешчаныя на бачным месцы, каб у іх можна было тыркнуць пальцам. Нават калі некаторыя рэчы падаюцца відавочнымі – усё адно надрукуйце іх ды павесьце на сьцяну. Проста гэта вельмі важны **псыхалягічны момант:** сказаць камусьці «нельга!» прасьцей, спаслаўшыся на правілы ці загад кіраўніцтва, чым адмовіць «ад сябе». Многія людзі ўвогуле ня ўмеюць адмаўляць, але кожны можа сказаць: «пачытайце правілы, вунь там, на сьцяне» – адмовіўшы такім ускосным чынам.

Як захоўваць папяровыя дакумэнты

Папера – праблема бясьпекі. Звычайна ў офісах няўрадавых арганізацыяў, дзе ёсьць шмат супрацоўнікаў, зьбіраецца шмат дзелавых папераў, якія колісь былі вельмі важныя, а пасьля страцілі сваю актуальнасьць і сталі нікому не патрэбныя – пра іх папросту забыліся. Але для спэцслужбаў і «сэксотаў» яны могуць уяўляць вялікую цікавасьць. Раздрукаваныя паперы з сакрэтнай інфармацыяй (альбо нават і зь несакрэтнай, простай працоўнай інфармацыяй) уяўляюць сабой небясьпеку, якой ня так проста пазбыцца, – героі клясычнай літаратуры палілі дакумэнты ў агні, аднак у наш час такі варыянт малаверагодны, дый паперы стала замнога. Не выкідайце важныя дакумэнты ў сьметніцу, «органы» могуць наняць пару бамжоў, якія будуць перабіраць сьметны бак, адбіраючы, апроч пустых пляшак, вашыя паперы. Вынішчайце дакумэнты, у тым ліку і чарнавікі. Просты варыянт – парваць на дробныя кавалкі і высыпаць іх часткамі ў розныя сьметніцы па дарозе дахаты (але і ў гэтым варыянце ня трэба недаацэньваць руплівасьць і апантанасьць некаторых шпегаў-фанатыкаў). Больш зручны і надзейны варыянт – «шрэдэр», здрабняльнік паперы. Гэты апарат наразае паперу на танюткія палосачкі і блытае іх. Аднавіць дакумэнт пасьля гэтага немагчыма.

Адным з небясьпечных момантаў у працы з дакумэнтамі зьяўляецца транспартаваньне дакумэнтаў. Зыходзячы з практыкі, менавіта падчас перамяшчэньня дакумэнтаў і важных папераў гэтыя матэрыялы могуць патрапіць у рукі спэцслужбаў.

Таму перасоўваньне дакумэнтаў у прасторы варта зьвесьці да мінімуму. Замест таго каб паўсюль насіць з сабою важныя дакумэнты, перасоўваючы іх з аднаго "бясьпечнага" месца ў іншае, "яшчэ больш бясьпечнае", і назад, варта вызначыць сталае месца захоўваньня альбо працы з гэтым дакумэнтам. Тут таксама можна кіравацца прынцыпам дэцэнтралізацыі - можна вызначыць некалькі надзейных месцаў захоўваньня для розных дакумэнтаў. Паверце, што ахранцы будзе цяжэй вызначыць, якая з трыццаці кватэр, якія вы наведалі за тыдзень, будзе вашым "архівам", чым лавіць вас пастаянна на выхадзе з "палёнай" штаб-кватэры вашай арганізацыі (само памяшканьне штаб-кватэры лепей увогуле пазбавіць будзь-якіх сакрэтных дакумэнтаў).

Ня варта насіць з сабой тыя паперы, якія непатрэбныя вам для дзейнасьці ў дадзены пэрыяд часу. Таксама ня варта захапляцца запаўнень-

нем нататнікаў важнай інфармацыяй - нататнік у выпадку затрыманьня можа згуляць супраць вас і нават стаць важным рэчавым доказам у крымінальнай справе (падчас аднаго з гучных судовых працэсаў у Беларусі ў якасьці асноўнага доказу супрацьпраўнай дзейнасьці абвінавачанага фігуравала ажно 13 нататнікаў з падрабязнымі зьвесткамі). Сканфіскаваны нататнік можа выкрыць вашыя кантакты. Таму паводле магчымасьці інфармацыю ў нататніках варта зьмяшчаць у кадаваным альбо незразумелым для чужога вока выглядзе (самаменш, можна рабіць запісы беларускай лацінкай). Пры запаўненьні нататніка (а таксама пры складаньні іншых дакумэнтаў) было б некепска ўявіць, што гэтыя дакумэнты патрапілі ў рукі спэцслужбаў і тыя іх аналізуюць, - зыходзячы з гэтага можна выправіць тыя моманты, якія зьяўляюцца найбольш небясьпечнымі. Нататнікі варта мяняць як мага часьцей, пазбаўляючыся ад састарэлых кантактаў і іншай інфармацыі, скарыстаныя нататнікі лепей зьнішчаць, а калі гэта немагчыма - здаваць на часовае захоўваньне ў кансьпіратыўны "архіў". У прынцыпе, надзейней усю інфармацыю, якая захоўваецца стала, пераводзіць у лічбавую кадаваную форму.

На дакумэнтах, якія могуць стаць падставай для абвінавачаньня ў зьдзяйсьненьні крымінальнага злачынства (напр. паклёп альбо зьнявага прэзыдэнта, заклікі з мэтай зьвяржэньня канстытуцыйнага ладу ды інш.) варта рабіць прыпіскі, якія б дэзавуявалі сэнс дакумэнту. Напрыклад, на плянах і праграмах можна ставіць надпісы: «Матэрыялы для дэтэктыўнага апавяданьня», «Праграма аб'яднаньня "Млада Фронта", Славаччына, 1929 г.» і г. д. Пад крытычнымі матэрыяламі на адрас прэзыдэнта і дзяржаўнай улады можна ставіць прыпіску: «…але ўсё гэта зьяўляецца няпраўдай і ня мае нічога агульнага з рэчаіснасьцю».

Прынамсі, варта распрацаваць простыя правілы працы з дакумэнтамі для вашай арганізацыі:

- раздрукоўваюцца толькі тыя канфідэнцыйныя дакумэнты, якія раздрукаваць неабходна;
- кожны дакумэнт мусіць мець гаспадара – асобу, якая адказная за яго выраб, працу зь ім і яго зьнішчэньне;
- непатрэбныя дакумэнты зьнішчаюцца ўва ўстаноўленым бясьпечным парадку (гэта датычыцца як канфідэнцыйных дакумэнтаў, так і бягучых дакумэнтаў і чарнавікоў);
- прызначаецца адказны за бясьпеку працы з паперамі.

Як вырабляць, захоўваць і распаўсюджваць друкаваныя матэрыялы

Пры працы з друкаванымі матэрыяламі трэба часава і тэрытарыяльна разьдзяляць фазы вырабу, захоўваньня і распаўсюду. Гэта значыць, што надрукаваны ў друкарні матэрыял не павінен адразу дастаўляцца на штаб-кватэру альбо на кватэру распаўсюднікаў. Пажадана мець кватэру-склад (лецішча, гараж, падсобка), дзе гэтыя матэрыялы будуць захоўвацца ў гуртоўным стане да перадачы на распаўсюд у раздроб. Адначасова на штаб-кватэры павінна быць такая колькасьць друкаваных адзінак, якую не шкада згубіць у выпадку нападу.

Асобы, не заангажаваныя ў выраб друкаванай прадукцыі, не павінны ведаць, дзе знаходзіцца падпольная друкарня. Асобы, якія не займаюцца захоўваньнем друкаванай прадукцыі, не павінны ведаць, дзе знаходзіцца склад улётак. Кожны мусіць ведаць свой участак працы і безь неабходнасьці не цікавіцца, што адбываецца за яго межамі.

Важным і асабліва небясьпечным пытаньнем зьяўляецца транспартаваньне друкаванай прадукцыі – гэтай працай павінны займацца альбо адмысловыя людзі, якія нічым больш не займаюцца, альбо надзейныя, але «незасьвечаныя асобы». На скрайні выпадак транспартаваньнем займаюцца самі актывісты. Пазьбягайце выкарыстаньня таксовак. Калі няма іншага выйсьця – ускладніце маршрут, мяняйце машыны, кожная новая таксоўка мусіць быць зь іншай фірмы ці таксапарку, але й нават пры такіх засьцярогах – гэта толькі разавы рэцэпт. Многія кіроўцы таксуюць у адных і тых жа месцах і хутка запомняць незвычайнага пасажыра. Міліцыя і спэцслужбоўцы часта «прачэсваюць» гэтую прафэсійную праслойку, пры гэтым яны могуць выставіць вас у ролі, напрыклад, забойцы ці ліхадзея, так што кожны таксоўца палічыць за абавязак вас «здаць».

Абсалютна недапушчальна транспартаваць незапакаваную ў непразрыстую абгортку прадукцыю – наклад мусіць быць надзейна запакаваны, каб не выклікаць залішніх зачэпак у чужога незацікаўленага вока. У друкарнях часта ставяць на пакункі пазнакі, нярэдка пішуць назвы кніжак. Папрасіце, каб яны не пісалі нічога апроч лічбаў ці ўмоўных знакаў альбо «кодавую назву» (кшталту «Как перестать беспокоиться и начать жить»).

Адкрытыя тэлефонныя размовы пра друкаваную прадукцыю павінны быць выключаныя, а кадаваныя размовы павінны быць зьведзеныя да мінімуму. У выпадку выкарыстаньня кодаў код трэба рэгулярна мя-

няць. Безь неабходнасьці ня трэба камунікаваць з падпольнай друкарняй: уладам ня так важна перахапіць канкрэтны наклад улётак, яны хутчэй хочуць увогуле спыніць непадцэнзурны друк на гэтай тэрыторыі. У ідэальным становішчы, рэдакцыя і падпольная друкарня ўвогуле не павінны камунікаваць паміж сабой – мусіць быць адмысловы сувязны, які перадае інфармацыю паміж імі. Таксама ня варта занадта часта камунікаваць праз тэлефон паміж рэзэрвовымі сховішчамі і іншымі элемэнтамі сыстэмы распаўсюду.

Самае горшае, што можна зрабіць, – наладзіць масавую выдачу ўсяго накладу матэрыялаў распаўсюднікам наўпрост на штаб-кватэры: для мянтоў самае зручнае – зрабіць засаду перад дзьвярамі офісу і перахопліваць распаўсюднікаў. З гэтай жа прычыны распаўсюд трэба пачынаць з тых раёнаў, што знаходзяцца ў далечыні ад штаб-кватэры.

Распаўсюднікі друкаваных матэрыялаў павінны мець пры сабе пасьведчаньні асобы, найлепей пашпарт, ня варта мець пры сабе зброю. Распаўсюднікі павінны працаваць «у полі» групай (2–5 чалавек) і мець «базу» – г. зн. чалавека, які носіць з сабой вялікую партыю накладу, трымаецца ўбаку ад распаўсюднікаў. Распаўсюднікі павінны мець пры сабе толькі мінімальную партыю (у выпадку з пэрыядычнымі выданьнямі – 200–300 асобнікаў), дастатковую для паўгадзіны-гадзіны працы. Калі ў распаўсюднікаў заканчваюцца матэрыялы, яны падыходзяць да «базы» і атрымліваюць новы пачак. Практыка паказвае, што пры дысцыплінаванай працы такі фармат дазваляе зьвесьці да мінімуму колькасьць матэрыялаў, якія трапляюць у лапы мянтам: патрулі, пабачыўшы распаўсюдніка, звычайна адразу імкнуцца схапіць яго. Гэтае правіла датычыцца распаўсюду друкаваных матэрыялаў на вуліцах, у транспарце і шляхам раскідкі па паштовых скрынях.

Калі распаўсюдніка затрымалі і даставілі ў пастарунак, ён не павінен панікаваць і павінен прытрымлівацца загадзя ўзгодненай інструкцыі аб паводзінах падчас затрыманьня. Перад пачаткам працы яму трэба давесьці, што за распаўсюд друкаваных выданьняў прадугледжаны адносна невялікі штраф. Зразумела, ня варта казаць, адкуль узяліся гэтыя друкаваныя матэрыялы (Хто даў? Колькі было атрымана і колькі пасьпеў распаўсюдзіць? Ці сам вырабляў або нехта даручыў? Якая арганізацыя займаецца вырабам і распаўсюдам?). Трэба памятаць, што распаўсюднік увогуле можа **адмовіцца ад будзь-якіх тлумачэньняў**, хоць гэта і патрабуе пэўнай псыхалягічнай загартоўкі. Таму распаўсюднікі павінны ведаць шэраг шаблонных «адмазак»: «Знайшоў на лаў-

цы ў сквэры, вырашыў параздаваць сябрам і мінакам», «Знайшоў на сьметніцы каля выканкаму» і г. д.

Важнае правіла: пасьля затрыманьня нельга адразу ісьці на «базу» альбо штаб-кватэру: існуе небясьпека прывесьці за сабой хваста.

Асобна адзначым вялікую папулярнасьць і досыць высокую эфэктыўнасьць гэтак званага **дэцэнтралізаванага** вырабу і распаўсюду друкаваных матэрыялаў. Гэта значыць, напрыклад, што актывістам па ўсёй краіне рассылаюцца праз электронную пошту (альбо зьмяшчаюцца на пэўным сайце ў Інтэрнэце) узоры матэрыялаў, актывісты іх памнажаюць саматужным спосабам (падпольныя друкарні і рызографы тут неабавязковыя, дастаткова хатняй друкаркі альбо партатыўнага ксэракса ў невялічкай арганізацыі) у колькасьці, якая ім неабходная для распаўсюджаньня ўласнымі сіламі. Дзякуючы гэткай тэхналёгіі можна распаўсюдзіць хутка і па ўсёй краіне досыць вялікі наклад. Пры гэтым ня маецца адзінага «цэнтру» вырабу, захоўваньня і распаўсюду, а таксама адсутнічае рызыка, што «тавар» перахопяць пры транспартаваньні.

Пры вырабе і транспартаваньні забароненых кніжак раім выкарыстоўваць дзедаўскую мэтодыку: вокладка кніжкі не павінна выклікаць аніякіх пытаньняў у «праваахоўнікаў» (кшталту «Самосовершенствование – дорога к успеху»), а пад ёй хаваецца недазволены зьмест (як вы бачыце ў *гэтым* выданьні). Пазьней «цнатлівую вокладку» можна зьняць.

Пры макетаваньні друкаванай прадукцыі трэба ўлічваць, што беларускае заканадаўства патрабуе разьмяшчэньня на друкаваных вырабах выхадных зьвестак і штрыхавога коду па форме ISBN (штрыхавы код у абавязковым парадку разьмяшчаецца на кнігах і брашурах на чацьвертым баку вокладкі). Для пэрыядычных выданьняў выхаднымі зьвесткамі лічацца назва выданьня, заснавальнік (заснавальнікі), імя і прозьвішча рэдактара (галоўнага рэдактара альбо ягонага намесьніка), парадкавы нумар выпуску і дата яго выхаду, кошт альбо паметка «Бескаштоўна» ці «Вольны кошт», наклад, поўныя адрасы рэдакцыі і друкарні, рэгістрацыйны нумар. Па магчымасьці гэтыя зьвесткі павінны разьмяшчацца на пэрыядычным выданьні (нават на тым, якое выдаецца з пазначаным накладам да 300 асобнікаў і не падлягае дзяржаўнай рэгістрацыі). Натуральна, пазначаны наклад усіх незарэгістраваных пэрыядычных выданьняў не павінен перавышаць 300 асобнікаў (гэта значыць, максімум – 299 асобнікаў). Для нелегальных пэры-

ядычных выданьняў, гэтаксама як і для падпольных кніг і улётак, мае сэнс пазначаць прыдуманыя каардынаты рэдакцыі і друкарні. Цяпер у Беларусі пашыраная практыка, калі выдавец прыдумвае нейкую друкарню з галавы ў нейкім экзатычным расейскім альбо ўкраінскім горадзе ці проста піша «Надрукавана ў Эўропе». Напэўна, тут можна проста цалкам перапісаць каардынаты друкарні зь нейкай расейскай кніжкі.

Як весьці размовы праз тэлефон

Падазрэньне, што спэцслужбы праслухоўваюць усіх, – адно з пашыраных грамадзкіх перакананьняў. Шмат хто лічыць гэта забабонам, спасылаючыся на вялізныя рэсурсы, якіх вымагае гэткая дзейнасьць. На самай справе ў гэтай тэзе шмат што адпавядае рэчаіснасьці, і маштабы праслухоўваньня сапраўды вялікія. Выкрытыя пасьля «памаранчавай рэвалюцыі» ўва Ўкраіне памеры праслухоўваньня тэлефонаў палітычных і грамадзкіх актывістаў паказваюць, што спэцслужбы не шкадуюць рэсурсаў на гэтую дзейнасьць – слухаюць усіх, чыя дзейнасьць іх цікавіць.

Калі вы карыстаецеся мабільным тэлефонам, то акрамя тэхнічных характэрыстыкаў мадэлі вам нельга забывацца пра чатыры іншыя якасьці гэтага прыстасаваньня: магчымасьць перадачы спэцслужбам інфармацыі пра месца знаходжаньня абанэнта; магчымасьць фіксацыі выходных і ўваходных тэлефанаваньняў; магчымасьць праслухоўваньня і запісу размоваў, а таксама SMS'ак; дыстанцыйнае ўключэньне мікрафона для праслухоўваньня нават пры выключаным апараце (апошняе не праверана, але і не абвергнута). У прынцыпе, гэтыя небясьпекі пашыраюцца на ўсе мадэлі тэлефонаў.

Адзінае галоўнае правіла, якім трэба кіравацца, – **тэлефон не прызначаны для размоваў**. Гэта парадокс павінны быць прынцыпам нелегальнай дзейнасьці.

Калі вам трэба высьветліць нейкае пытаньне, то выкарыстоўвайце **тэлефон не для размовы, а для таго, каб дамовіцца пра час і месца размовы**, таксама ў кадаваным выглядзе. Асабліва гэта правіла датычыцца мабільных тэлефонаў вядомых грамадзкіх актывістаў (некаторыя зь іх кіруюцца правілам «Ну і няхай слухаюць» – і такім чынам даюць спэцслужбам карысную інфармацыю, якая можа быць скарыстаная пазьней ня толькі супраць іх саміх, але і супраць іх карэспандэнтаў). Лепей дамаўляцца кадаванымі словамі альбо словамі, зразуме-

лымі толькі вам, кшталту «Варыянт С», «Там жа, дзе і пазаўчора», «На прыпынку», «Ля школы», «Пад гадзіннікам». Замест таго каб казаць: «У кавярні “Вавёрачка” – лепей выкарыстаць код альбо сказаць: «У кавярні на Партызанскім» ці «Ну, памятаеш, на Мотавела…» Асабліва пільнымі ў гэтым сэнсе трэба быць падчас маштабных акцыяў, важных сустрэчаў і перамоваў, выбарчых і іншых палітычных кампаніяў. SMS-паведамленьні такія ж небясьпечныя, імі таксама трэба абменьвацца асьцярожна, з выкарыстаньнем коду. Сачыце, каб у памяці вашага мабільніка не было лішніх SMS’ак (на выпадак адабраньня мабільніка). Памятайце, што спэцслужбы часта зважаюць на колькасьць званкоў з аднаго тэлефона на іншы: напрыклад, калі «пад каўпаком» знаходзіцца апазыцыйны дзяяч, то аўтаматычна зьвяртаецца ўвага на тыя нумары, на якія ён часьцей за ўсё тэлефануе (з хатняга і мабільнага тэлефона). Напрыклад, калі дзяяч, які знаходзіцца ў прыярытэтным сьпісе праслухоўваньня, патэлефанаваў чалавеку першы раз у жыцьці (нават памыліўся нумарам), то гэты абанэнт аўтаматычна на трапляе ў калектыўную памяць органаў і ўжо ня будзе забыты.

Падчас канфідэнцыйных і важных размоваў мабільны тэлефон трэба адключаць і вымаць батарэю (найлепей зрабіць гэта загадзя, ня ў тым месцы, дзе адбываюцца перамовы). Заўжды добра, калі вы ня возьмеце з сабою тэлефона, калі пойдзеце на сустрэчу: памятайце, што праз мабільны тэлефон нескладана вылічыць вашае месца знаходжаньня (дакладнасьць можа быць высокай: ажно да нумару дому). Пакіньце мабільнік у офісе ці дома (адключаным альбо ўключаным) – і ідзіце на сустрэчу. Калі вам асабліва каштоўная канфідэнцыйнасьць – па-магчымасьці рэгіструйце мабільныя тэлефоны на іншых, незасьвечаных асобаў (а таксама можна карыстацца карткамі замежных апэратараў з роўмінгам). Але ўлічвайце, што ў мабільных сетках рэгіструецца ня толькі SIM-картка, але й тэлефонны апарат,– таму для новых і замежных SIM-картак лепей выкарыстоўваць новыя апараты. Практычная заўвага: калі батарэі вашага тэлефона звычайна хапала на пяць дзён размоваў, а раптам яна стала разраджацца за дзень – верагодна, што ў вашым тэлефоне працуе «жучок», хаця, магчыма, проста прыйшоў час замяніць акумулятар.

Лепей не праводзіць сакрэтныя размовы ў пакоі, дзе ёсьць стацыянарны тэлефон (ён можа выкарыстоўвацца як сталае прыстасаваньне праслухоўваньня).

Адзначым, што існуе некалькі сродкаў абароны ад праслухоўваньня

тэлефонных размоваў. У прынцыпе, усе яны вымагаюць прыцягненьня спэцыяліста, аднак некаторыя даступныя ў продажы і могуць быць скарыстаныя і «чайнікамі».

Самым простым варыянтам зьяўляецца набыцьцё **скрэмблера** – прылады для кадаваньня размовы, якая кадуе сыгналы перад іх перадачай. Плюсам зьяўляецца тое, што скрэмблер дазваляе мець дастаткова высокую ступень шыфраваньня размовы – ён можа абараніць ад любога зь відаў праслухоўваньня і стацыянарнага тэлефона, і мабільніка (пры гэтым, натуральна, трэба папярэдне рабіць праверку ўсяго памяшканьня: вас могуць слухаць і пры дапамозе «жучка»). Мінус – абодва абанэнты павінны мець сумяшчальныя скрэмблеры, – так што гэтую схему рацыянальна выкарыстоўваць для тых абанэнтаў, якія пастаянна вядуць паміж сабой канфідэнцыйныя размовы. Гэтая тэхналёгія шырока прадстаўленая на рынку, а ваганьне коштаў – ад 500 да некалькіх тысячаў даляраў – залежыць ад надзейнасьці выкарыстаных для шыфраваньня альгарытмаў.

Апошнім часам вялікую папулярнасьць набылі гэтак званыя **крыптафоны**. Па-сутнасьці, гэта мадэлі тэлефонаў з убудаваным скрэмблерам вялікай магутнасьці. Заўважым, што адным з сцэнароў выкарыстаньня крыптафона яго вынаходнікі называюць «выкарыстаньне праваабарончымі няўрадавымі арганізацыямі». Аднак, на бягучы час гэта хутчэй тэарэтычны варыянт для нас, бо такая апаратура задорага каштуе (вядзецца пра тысячы эўра). Зрэшты, калі для вас гэта не праблема вось спасылка: www.cryptophone.de.

Больш цікавым падаецца выкарыстаньне IP-тэлефаніі з шыфраваньнем. Памянёная ай-пі-тэлефанія – гэта, кажучы проста, размовы (менавіта голасам) праз Інтэрнэт. Гаворыш у мікрафон далучаны да свайго кампутара, суразмоўца чуе сказанае з дынамікаў свайго кампутара. Розьніцы паміж гукам, карцінкай ці дакумэнтам для электроннай тэхнікі няма -- усё гэта можа быць пераведзенае ў лічбавую форму і дасланае праз сусьветнае Сеціва. І, канечне ж, можа быць зашыфраванае. Добравядомы ў гэтай галіне сродак – **PGPFon**.

Існуюць прылады, прызначаныя для зьнішчэньня альбо выяўленьня «жучкоў» у памяшканьнях, аўтамабілях, на тэлефонных ды электрадратах. Яны, на жаль, каштуюць немалых грошай і вымагаюць досьведу, якога ў вас хутчэй за ўсё няма. Апроч таго, у гэтай сфэры ўсё імкліва разьвіваецца, так што, калі ў вас няма свайго (вартага даверу) адмыслоўцы, то лепш проста не абгаворвайце сакрэтных справаў у «па-

паленых» памяшканьнях. Ня трэба ствараць сталых месцаў для перамоваў, улічвайце, што кавярні і рэстарацыі – зручныя для праслухоўваньня месцы, у якіх (хаця б і выпадкова) могуць аказацца варожыя вушы.

Пераезд праз мяжу

Лепей устрымацца ад перавозу праз мяжу канфідэнцыйных, сакрэтных і проста важных дакумэнтаў, а таксама буйных сумаў наяўных грошаў. Калі гэтага нельга пазьбегнуць, то дакумэнты варта правозіць у выглядзе зашыфраванай электроннай вэрсіі (гл. заўвагі пра рэзэрвовыя копіі). Майце на ўвазе, што мытнікі маюць тэхнічныя магчымасьці для прагляду электронных носьбітаў. Тэарэтычна, яны могуць не прапусьціць яўна зашыфраваную інфармацыю. Абавязкова трэба карыстацца крыптаграфіяй (шыфраваньнем), а найлепей, каб не выклікаць залішніх падазрэньняў, – стэганаграфіяй (гл. вышэй).

Можна адзначыць, што ў мабільнікі, аснаджаныя такімі функцыямі, як інфрачырвоны порт альбо bluetooth, у прынцыпе, можна запісаць ня толькі мэлёдыю альбо застаўку, але й любы файл (прынамсі, для многіх мадэляў). Памер файлу абмежаваны свабоднай памяцьцю тэлефона, але можа аказацца дастатковым для некаторых дакумэнтаў (зразумела ж, у зашыфраваным выглядзе). Загадзя прадумайце, як вы будзеце «даставаць» файл з свайго сотавага сябра, для гэтага: 1) у тэлефоне мусіць быць функцыя «выслаць праз інфрачырвоны порт (альбо bluetooth)»; 2) спатрэбіцца кампутар, здольны прымаць файлы праз той жа порт (сучасныя ноўтбукі звычайна гэта могуць). Надзейнасьць такога спосабу яшчэ вымагае ацэнкі. У прынцыпе, амаль у любы мабільны тэлефон можна закачаць пэўную колькасьць інфармацыі з дапамогай камунікацыйнага кабелю. А яшчэ зручней для перавозу інфармацыі праз мяжу карыстацца мр3-плэерамі і лічбавымі фотаапаратамі, якія абсалютна легальна могуць утрымліваць некалькі соцень мегабайтаў альбо нават гігабайтаў інфармацыі і не выклікаюць залішніх падазрэньняў. Для стороньняга вока гэта проста плэер (яго і слухаць трэба, а ня толькі інфармацыю праз мяжу вазіць) альбо звычайны фотаапарта (колькі іх перасякае мяжу за дзень!).

Беларускае заканадаўства дазваляе ўвозіць у краіну без дэкляраваньня суму, эквівалентную 3000 даляраў ЗША, але калі сума большая, то яна падлягае абавязковаму дэкляраваньню. Паходжаньне грошай

пазначаць ня трэба. Трэба, аднак, ведаць, што зьвесткі пра дэкляраваньне потым трапляюць у падатковую інспэкцыю і розныя правяраючыя органы, таму пазьней тыя могуць пачаць расьсьледаваньне – што гэта за грошы, ці сплачаныя зь іх падаткі? Але пры перасячэньні мяжы ніякіх дакумэнтаў ня трэба. Што тычыцца расейска-беларускай мяжы, дык праз яе дазволена правозіць любую колькасьць валюты без аніякага дэкляраваньня. Аднак на іншых межах недэкляраваныя грошы, па-першае, канфіскуюць, па-другое, могуць нават распачаць крымінальную справу аб кантрабандзе.

Пры дэкляраваньні грошай ні ў якім разе нельга пазначаць, што яны вязуцца для мэтаў няўрадавай арганізацыі (бяз розьніцы, зарэгістраванай альбо незарэгістраванай) альбо дзеля мэтаў гуманітарнае дапамогі.

Не забывайцеся, што ў Беларусі існуе некалькі ступеняў кантролю за перасоўваньнем грамадзянаў праз мяжу. Існуе сьпіс асобаў, перасоўваньне якіх праз мяжу адсочваецца, а ў дачыненьні да некаторых асобаў стала выкарыстоўваецца асабісты дагляд (асобы, якія перасякаюць мяжу разам з гэтымі людзьмі, таксама трапляюць у кантрольны сьпіс). Таму без асаблівай неабходнасьці ня варта афішаваць на мяжы сваю датычнасьць да вядомых дзеячоў, да якіх скіраваная пільная ўвага памежнікаў і мытнікаў.

На мяжы мытнікі маюць права правесьці ня толькі дагляд рэчаў, але і асабісты дагляд, і дагляд транспартнага сродку. У выпадку калі ў транспартным сродку будзе знойдзеная будзь-якая кантрабанда, нават калі гэта цыгарэты ці піва, транспартны сродак можа быць сканфіскаваны. Асабісты дагляд можа выкарыстоўвацца толькі на асабісты загад начальніка мытнага паста. Асабісты дагляд патрабуе складаньня пратаколу дагляду і павінны адбывацца ў спэцыяльна прыстасаваным памяшканьні ў прысутнасьці панятых таго ж полу, што і вы. Калі вы ня маеце пры сабе анічога крамольнага і вам прапануюць прайсьці асабісты дагляд – не лянуйцеся, патрабуйце выкананьня ўсіх фармальнасьцяў працэдуры, гэтым вы можаце дапамагчы іншым людзям.