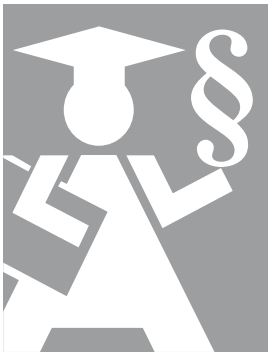
МЕН № 4 (88), серпень, 2016 р.



МЕТОДИЧНІ РЕКОМЕНДАЦІЇ НОТАРІАЛЬНОЇ ПАЛАТИ УКРАЇНИ ЩОДО ДІЙ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОГО ХАРАКТЕРУ ДЕРЖАВНИХ ТА ПРИВАТНИХ НОТАРІУСІВ УКРАЇНИ У СФЕРІ БЕЗПЕКИ ВИКОРИСТАННЯ ЄДИНИХ ТА ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ

ПЕРЕДМОВА

Цей матеріал зібрано, проаналізовано та представлено Комісією Нотаріальної палати України з питань запобігання та протидії кіберзлочинності з метою убезпечення мінімальними особистими зусиллями кожного з Вас від несанкціонованого використання електронно-цифрових підписів (ключів ЕЦП) до Єдиних та Державних реєстрів. Виконання всіх нижченаведених рекомендацій не надасть 100% гарантії від крадіжки Ваших ключів, однак кожен з Вас сам приймає рішення, чи потрібно йому перевірити свою електронну машину, безпеку ключів і всіх даних Вашого комп'ютера.

Ці рекомендації визначають кроки для підтримання належного рівня інформаційної безпеки нотаріального офісу з метою запобігання перехоплення третіми особами через Інтернет інформації, що становить нотаріальну таємницю, а також ідентифікаторів доступу до Єдиних та Державних реєстрів.

Час не стоїть на місці, світ розвивається і ми розвиваємося. Технології випереджають навіть наші припущення. Поки ми думаємо, як убезпечити себе, хтось вже придумав, як зламати нашу оборону.

Найбільша помилка нотаріусів — це те, що Ви копіюєте ключі на кілька флеш-носіїв, здійснюєте вхід до реєстрів з декількох комп'ютерів. Крім того, має місце людський фактор — помічники і довірені особи, які користуються Вашими ключами.

Друга помилка — це відсутність на Ваших комп'ютерах актуальних (оновлених) операційних систем та антивірусних-антишпигунських програм.

Також є помилкою зберігання паролів доступу до реєстрів у відкритих місцях, у тому числі в MICROSOFT WORD файлах, на «робочих столах» операційної системи Windows. Такі файли з паролями та ключами в першу чергу знаходять і копіюють зловмисники.

Відкритий доступ до офісної мережі WI-FI — це пряма дорога до комп'ютера нотаріуса.

Сподіваємося, що нижчевикладений матеріал допоможе посилити захист рівня інформаційної безпеки нотаріального офісу і надалі спокійно та впевнено працювати.

Президент
Нотаріальної палати України ***В.М. Марченко***

І. НАЙПОШИРЕНІШІ МЕТОДИ ВИКРАДЕННЯ ІНФОРМАЦІЇ (ЗЛАМУ ПАРОЛІВ)

1. Атака з використанням словників (наборів слів — варіантів паролів)

При цьому використовується простий файл, який містить слова-варіанти паролів. Іншими словами, атаки такого типу перебирають саме слова, які багато людей використовують як пароль. Така «хитрість», як вміло згруповані разом слова, наприклад, «сімсімоткройся» або «ясуперадміністратор», не врятують пароль від злому, можливо, хакери лише витратять кілька зайвих секунд.

2. Атака методом повного перебору (грубої сили)

Цей метод схожий на атаку за словником, але з додатковим бонусом (звичайно, для хакера). Він дозволяє виявити слова, що не містяться в словнику, перебираючи всі можливі букви і цифри комбінації від AAA1 до zzz10. Це не швидкий спосіб, особливо, якщо ваш пароль складається з декількох символів, але в кінцевому рахунку пароль буде розкритий. Метод повного перебору може бути спрощений за допомогою використання додаткових обчислювальних потужностей Вашого комп'ютера. При застосуванні цього метода можуть бути використані інші зламані комп'ютери.

3. Фішинг

Найпростіший спосіб злому — запитати у користувача його/її пароль. Фішингові повідомлення отримує та надає сам читач сайтів, це дає можливість вкрасти Ваш ключ, якій вставлений у порт USB комп'ютера, на підроблених сайтах онлайн-банкінгу, платіжних систем або інших сайтах, на яких потрібно обов'язково ввести особисті дані, щоб «виправити якусь страшну проблему з безпекою». Навіщо ускладнювати собі життя зломом пароля, коли користувач з радістю повідомить його сам? Цей спосіб зараз найчастіше використовується зловмисниками для отримання конфіденційної інформації.

4. Соціальна інженерія

Соціальна інженерія дотримується тієї ж концепції, що і фітинг, — «запитати у користувача пароль», але не за допомогою поштової скриньки, а в реальному світі. Улюблений трюк соціальної інженерії — зателефонувати в офіс під виглядом співробітника ІТ-безпеки і попросити пароль доступу до мережі. Ви будете здивовані, але це часто працює. Деякі злочинці навіть відчувають потребу надіти костюм і бейдж перш, ніж прийти в компанію, щоб звернутись до адміністратора в приймальні з таким проханням.

5. Шкідливе програмне забезпечення

Програма перехоплення вводу з клавіатури може бути встановлена шкідливим програмним забезпеченням, яке фіксує всю інформацію, яку Ви вводите, або створює скріншоти під час процесу авторизації, а потім надсилає копію цього файлу хакерам. Деякі шкідливі програми шукають існуючий файл з паролями користувача, потім копіюють цей файл, який (крім добре зашифрованих) буде містити легкодоступні збережені паролі з історії сторінок, відвіданих користувачем.

6. Підглядання через плече

Найбільш самовпевнені хакери під виглядом кур'єрів, фахівців технічного обслуговування кондиціонерів або будь-яких інших службовців проникають в офісні будівлі. Як тільки вони потрапляють в офісну будівлю, уніформа обслуговуючого персоналу надає їм свого роду безкоштовний квиток на безперешкодний доступ в усі куточки офісної будівлі. Це дозволяє їм записувати паролі, що вводяться реальними співробітниками, а також надає відмінну можливість побачити всі паролі, які вони так люблять писати на стікери і клеїти на монітори своїх комп'ютерів. У тому числі такі особи під виглядом клієнта можуть з'явитись до нотаріуса і помічника з проханням перевірити у реєстрах інформацію та знімати весь процес роботи нотаріуса або помічника на скриту відеокамеру і потім, розібравши відеоряд, зможуть отримати комбінації натиснутих клавіш тощо.

МЕН № 4 (88), серпень, 2016 р.

7. Припущення

Кращим другом зломщиків паролів, звичайно, є передбачуваність користувачів. Якщо дійсно випадковий пароль був створений за допомогою програмного забезпечення, призначеного для цього завдання, то для користувача випадковий пароль навряд чи буде нагадувати щось подібне. Замість цього, завдяки нашій емоційній прихильності до речей, які нам подобаються, швидше за все, ті «випадкові» паролі, які ми створимо, будуть засновані на наших інтересах, хобі, іменах домашніх тварин, сім'ї тощо. Насправді, паролі, як правило, будуються на основі всіх тих речей, про які ми так хотіли б поговорити в соціальних мережах і навіть включити в наш профіль. Зломщики паролів, цілком ймовірно, подивляться на цю інформацію і зроблять кілька, часто правильних, здогадок при спробі зламати пароль споживчого рівня, не вдаючись до словника або методу грубої сили.

II. СТАДІЇ ЗЛАМУ ОТРИМАННЯ КЛЮЧІВ ТА ПАРОЛІВ ДОСТУПУ ДО ЄДИНИХ ТА ДЕРЖАВНИХ РЕЄСТРІВ

Представники лабораторії комп'ютерної криміналістики CyberLab (http://cyberlab.com.ua/) виділяють такі стадії злому.

Перша стадія атаки включає розсилку на електронні адреси нотаріусів «фітингових» листів, які начебто надходять від імені Міністерства юстиції України, Головних територіальних управлінь юстиції, Нотаріальної палати України з незначною зміною справжніх адрес реальних відправників (наприклад, одна літера чи один знак), які містять вкладений файл (прикріплений файл), що містить шкідливі функції. При відкритті цього файлу відбувається зараження комп'ютера шкідливим програмним забезпеченням, а зловмисник отримує фактичне віддалене управління Вашим комп'ютером і спостереження за ним, включаючи можливість запису відеоряду (скріншотів) екрану, а також доступ до будь-яких файлів комп'ютера.

На **другій стадії** зловмисник вручну проводить моніторинг дій нотаріуса з метою перевірки наявності на зараженому комп'ютері програм і облікових даних доступу до Єдиних та Державних реєстрів.

У разі виявлення такої інформації проводиться **третя стадія** атаки — викрадення пароля та електронного цифрового ключа доступу. Для крадіжки логіна і пароля використовується кейлогер (*програма, яка реєструє всі натискання на клавіатуру*). Файл цифрового ключа крадуть під час прихованого віддаленого підключення, коли нотаріус підключає носій з ключем (зазвичай флешку) до комп'ютера. Файл має однакову і єдину назву key-6.dat, що робить його пошук дуже швидким і простим.

На **четвертій стадії** зловмисник, використовуючи викрадені облікові дані, здійснює фактичний доступ до Державного реєстру речових прав на нерухоме майно та вносить несанкціоновані зміни від імені нотаріуса. Коригування зводяться до заміни одного власника того чи іншого майна на іншого. Так легко і витончено українців позбавляють їх власності.

III. ОЗНАКИ МОЖЛИВОГО ЗЛАМУ КОМП'ЮТЕРА ТА ЙОГО ЗАРАЖЕННЯ ШКІДЛИВИМИ ПРОГРАМАМИ

1. Істотне уповільнення роботи

Багато вірусів-шпигунських програм, після того як проникли на Ваш комп'ютер, постійно працюють приховано, шукаючи можливості виконати своє злісне завдання або розповсюдитись. Вони можуть помітно погіршити і уповільнити роботу Вашого комп'ютера, особливо старих (не оновлених) операційних систем, а також подовжити час запуску комп'ютера. Це відбувається через те, що всі дії користувача фіксуються і відсилаються зовні. Після включення комп'ютера, не запускаючи жодних програм, спостерігайте за навантаженням операційної системи (завантаження процесора, жорсткого диска, навантаження на мережу) за допомогою стандартного «диспетчера завдань Windows».

2. Неможливо видалити деякі файли

Одне із завдань супротивника — вижити на ворожій території. Тому багато шкідливих

програм перешкоджають своєму видаленню. Якщо ви не можете видалити підозрілий файл на комп'ютері, на флешці або ж після видалення він відразу ж з'являється на старому місці, то цей файл варто перевірити антивірусною програмою або за допомогою сервісу https://www.virustotal.com/. Звертайте увагу на нові файли і папки, яких ви не створювали, особливо з дивними іменами, що складаються з літер і цифр.

3. Комп'ютер повністю або частково заблокований

Існують шкідливі програми, які повністю або частково блокують системні функції, протидіючи своєму виявленню. Наприклад, може бути заблокований диспетчер задач, панель управління, редактор реєстру, запуск антивірусу тощо. Так само викликає підозру несподівано відключений антивірус, або якщо при його запуску виникають помилки. Шкідливі програми можуть несподівано втручатись у роботу Вашого комп'ютера. Наприклад, так звані «трояни» можуть цілеспрямовано захопити веб-браузер з метою не допустити Вас на певні веб-сайти або не дати встановити певне програмне забезпечення. Також шкідливі програми можуть діяти спонтанно, наприклад, коли завантаження у комп'ютера мінімальне, тобто в той час, коли користувач з ним не працює і не зверне увагу на миттєве навантаження комп'ютера.

4. Втрата даних

З самого початку розробники комп'ютерних вірусів мали на меті стирати дані з машин безпомічних користувачів. Гарною новиною є те, що таких вірусів усе ж таки меншість. Однак певний ризик все ж існує, тому якщо Ваш комп'ютер вразить такий тип вірусу, Ви як мінімум проведете якусь частину часу, відновлюючи збережені дані.

5. Підозріло високий вихідний інтернет-трафік

Якщо ви помітили незвично велику кількість вихідного мережевого трафіку (зокрема, проявляється, коли комп'ютер працює і підключений до Інтернету, але Ви ним не користуєтесь), то комп'ютер, можливо, уражений. Такий комп'ютер може використовуватися для прихованої розсилки спаму або для розмноження мережевих черв'яків, або ж дані з Вашого комп'ютера пересилаються зовні.

6. Підвищена активність жорстких дисків або підозрілі файли в кореневих директоріях

Зловмисники після злому комп'ютера проводять сканування комп'ютера на предмет цікавих їм документів (файлів), у тому числі з інформацією, що містять логіни, паролі, контакти, фінансові дані тощо. Деякі мережеві черв'яки схожим чином шукають на диску файли з електронними адресами (email), що згодом використовуються для розсилки заражених листів. Якщо Ви помітили значну активність жорстких дисків, навіть коли комп'ютер стоїть без роботи, а в загальнодоступних папках (каталогах, теках) стали з'являтися файли з підозрілими назвами, це також може бути ознакою злому комп'ютера та зараження операційної системи шкідливою програмою. Підвищена активність жорстких дисків може бути викликана дефрагментацією таких дисків. Цей процес переважно проводить операційна система автоматично, і він не є шкідливим.

7. Антивірусна-антишпигуська програма, встановлена на Вашому комп'ютері постійно повідомляє про знайдені на комп'ютері шкідливі програми або файли, хоча в іншому все працює нормально

Хоча хакерські атаки можуть бути складними і незвичайними, більшість зломщиків покладається на добре відомі «трояни». Ці шкідливі програми дозволяють отримати повний контроль над зараженим комп'ютером. Якщо антивірус повідомляє про виявлення подібних шкідливих програм, то це може бути ознакою того, що Ваш комп'ютер відкритий для несанкціонованого віддаленого доступу.

IV. РЕКОМЕНДАЦІЇ З БЕЗПЕКИ ВАШОГО КОМП'ЮТЕРА

1. Налаштування операційної системи

– Антивірус та фаєрвол (*фільтр, який стежить за вихідним і вхідним трафіком, тобто, за всім, що Ваш комп'ютер отримує і надсилає, та повідомляє Вас про підозрілі*

дії, щоб ви приймали рішення, дозволяти їх чи ні) має бути на кожному робочому комп'ютері, постійно оновленим та ввімкненим.

– Заборонити автоматичний запуск компакт-дисків, інших носіїв інформації (бекап-дисків, флеш-дисків, карт пам'яті тощо).

Для ОС Windows7:

«Пуск» – «Панель управління» – «Автозапуск» – зняти прапорець з «Використовувати автозапуск для всіх носіїв і пристроїв»

– Слідкувати за тим, щоб вона систематично оновлювалась.

Для ОС Windows7:

«Пуск» – «Панель управління» – «Центр оновлення Windows» – «Увімкнути автоматичне встановлення оновлень»

– Для звичайної роботи з реєстрами та документами в операційній системі Windows рекомендовано створити окремий обліковий засіб, який не буде мати прав адміністратора. Тобто під користувачем з правами «Адміністратор» ви лише налагоджуєте операційну систему та встановлюєте програми, а під створеним користувачем з повноваженнями «Користувач» ви звичайно працюєте. Це не дозволить зловмиснику, який навіть отримає віддалений доступ до комп'ютера, здобути адміністративні права, а також такий механізм захисту у 90% не дасть шкідливим програмам без Вашого відома встановитись та автозавантажуватись.

Для ОС Windows7:

«Пуск» – «Панель управління» – «Облікові записи користувачів» – «Управління іншим обліковим записом» – «Створення облікового запису»

2. Паролі

– Періодично змінювати паролі користувачів на всіх комп'ютерах, а також пароль користувача (верхній пароль — пароль користувача) для доступу до реєстрів Національної інформаційної системи (НАІС);
– вхід (авторизація) у поштові сервіси має дворівневим, тобто вхід має відбуватись за допомогою генератора коду (https://lastpass.com/uk/) або надсилання коду на телефон;
– пароль має бути складним (мати довжину більше 6 символів), не містити особистих даних, повинен містити букви різних регістрів (великі, малі), хоча б одну цифру, та не бути звичайним словом (ялинка, кефір, нотаріус тощо).

Для того щоб не забувати паролі, можна використовувати електронний менеджер паролів http://keepass.info/, або ж створити окремий записник паролів і зберігати його виключно у сейфі.

Приклад складання пароля

Берете якийсь вірш чи рядок з пісні: «В лесу родилась елочка в лесу она росла». З цих рядків беремо перші та останні букви слів та записуємо їх у різних регістрах: ВЛуРьЕаВлУоНрА. Замінюємо букву «а» на символ «@» і отримуємо такий пароль: ВЛуРьЕ@ВлУоНр@
Перевірити пароль на складність підбору (зламу) можна на сервісі http://www.passwordmeter.com/, **наприклад, пароль** ВЛуРьЕ@ВлУоНр@ дуже сильний, але це не означає, що всі, хто прочитав цей абзац, мають його використати.

3. Користування інформацією

– Якщо Вам надійшов електронний лист з прикріпленим документом (файлом), який необхідно відкрити, слід продивитись вміст файлу за допомогою попереднього перегляду поштового сервісу (наприклад, gmail.com дозволяє це зробити). Якщо немає можливості попереднього перегляду, то цей файл слід завантажити, але не відкривати, перед відкриттям обов'язково перевірити його (файл) за допомогою https://www.virustotal.com/.

– Надавати перевагу веб-сайтам (веб-сервісам), що використовують шифрування (можна перевірити, але не завжди, через наявність «замочка» в адресному рядку браузера; точно перевірити чи має сайт сертифікат і використовує шифрування через сервіс https://www.ssllabs.com/ssltest/). «Замочок» означає, що цей сайт використовує шифрування. Отже, інформація, яка передається від Вас до сайту і від сайту до Вас, зашифрована. Якщо хтось по дорозі, поки йде інформація, перехопить Ваші дані, то він не зможе їх переглянути, оскільки для цього потрібен ключ.
– Не варто необдумано переходити за посиланнями, зазначеними в підозрілих листах.
– Якщо Вам пропонується інсталювати невідомий файл (програму) або маєте будь-який сумнів, то натискайте кнопку «скасувати», «ні» або ж закрийте вікно, в якому це пропонується.
– Для власної безпеки не варто використовувати поштові сервіси (Yandex, Rambler, Mail.ru), що базуються на території Російської Федерації.

4. Доступ до комп'ютера

– Унеможливіть фізичний доступ сторонніх осіб до комп'ютерів нотаріального офісу, а також не використовуйте на власних комп'ютерах сторонні носії інформації (карти пам'яті, флешки, диски).

Установіть вхід до операційної системи через введення пароля.

Для ОС Windows7:

«Пуск» – «Панель управління» – «Облікові записи користувачів» – «Створення пароля облікового запису».

Для ОС WindowsXP:

«Пуск» – «Панель управління» — «Облікові записи користувачів» – «Створення пароля».

– Блокуйте комп'ютер перед відходом від робочого місця.

Для ОС Windows7:

«Пуск» – натиснути стрілку праворуч від кнопки «Завершення роботи» у нижній частині меню Пуск – «Блокувати».

Для усіх ОС Windows:

натиснути одночасно на клавіатурі клавіші «Windows» та «L».

– Забороніть/обмежте використання чужих накопичувачів інформації (флеш-накопичувач, бекап-диск, компакт-диск, карти пам'яті тощо). Якщо все ж таки необхідно їх використати, то обов'язково перевірте такий носій інформації на відсутність шкідливих програм (вірусів), після чого скопіюйте необхідну інформацію на локальний диск і одразу вийміть сторонній носій інформації із комп'ютера.

5. Блокування доступу до Вашої робочої локальної мережі або мережі Wi-Fi:

а) доступ до локальної мережі мають виключно комп'ютери та техніка Вашої мережі;
б) якщо ви використовуєте мережу Wi-fi, то до неї можуть мати доступ виключно комп'ютери та техніка Вашої мережі;
в) якщо Вашим клієнтам необхідний доступ до Інтернету або до принтера, надайте цей доступ через окрему (гостьову) мережу Wi-fi або безпосередньо приєднайте принтер до ноутбука клієнта.

6. Використовуйте останні версії програмного забезпечення (ПЗ), патчі, оновлення. Виробники ПЗ постійно випускають оновлення для виправлення відомих вразливостей. Тримайте операційну систему, офісну програму, антивірусну-антишпигунську програму в актуальному стані (оновлену), щоб запобігти нападникам (кіберзлочинцям) здійснювати протиправні дії — втручання у Вашу інформаційну мережу за допомогою використання таких вразливостей.

7. Відключайте в операційній системі функцію віддаленого доступу, а також вимикайте автоматичне завантаження сторонніх програм, що дозволяють віддалене управління комп'ютером. Деякі операційні системи та сторонні програми надають функціонал для віддаленого моніторингу Вашого комп'ютера, у тому числі веб-сторінку.

МЕН № 4 (88), серпень, 2016 р.

8. Закривайте програми Єдиних та Державних реєстрів, коли не використовуєте їх, не залишайте комп'ютери без нагляду з увімкненими програмами реєстрів, не залишайте носії інформації з ключами ЕПЦ у комп'ютерах, коли їх не використовуєте.

9. Використовуйте на комп'ютерах **фаєрвол (мережевий екран, брандмауер) — програму, яка здійснює контроль і фільтрацію мережевих пакетів, що проходять через неї відповідно до заданих правил.**

Основним завданням фаєрвола є захист від несанкціонованого доступу.

Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання — не пропускати (фільтрувати) пакети, що не підходять під критерії, визначені в конфігурації.

За допомогою фаєрволу можна дозволити доступ до мережі Інтернет лише виключним програмам.

На комп'ютері у нотаріальному офісі рекомендуємо дозволити доступ до Інтернету лише реєстрам НАІС, веб-браузерам, антивірусу, операційній системі.

Також налагодити фаєрвол на роботу, при якій кожен доступ окремої програми має бути санкціонований користувачем, тобто, якщо програма хоче отримати доступ до Інтернету, то фаєрвол повідомить Вас про це і запитає про надання дозволу.

Використання фаєрволу унеможливлює анонімний доступ шкідливих програм як іззовні до Вашої мережі, так і навпаки.

Перелік безкоштовних фаєрволів

Outpost Firewall Free

Comodo Firewall

ZoneAlarm Free Firewall

PC Tools Firewall Plus

Додаток 1

ПАМ'ЯТКА НАІС
(Додаток 3 до Договору про надання послуг з підключення та забезпечення технічної підтримки користування Єдиними та Державними реєстрами)

1. Загальні положення

В якості носіїв ключової інформації, що використовуються в Єдиних та Державних реєстрах (далі — Системи), застосовуються такі носії даних:

- для розміщення Особистих ключів користувачів — зовнішній носій даних типу CD-R, DVD-R або flash-memory;
- для розміщення посилених сертифікатів відкритих ключів користувачів — жорсткі диски ПЕОМ.

ЕЦП призначений для здійснення авторизації користувача при його вході в Систему згідно з відповідною Інструкцією з користування Системою.

2. Обов'язки користувача Системи

При роботі в Системі користувач зобов'язаний:

- зберігати Особистий ключ, носій ключової інформації, на якому він розміщений, та пароль доступу до нього у таємниці, не допускати використання Особистого ключа іншими особами;
- не використовувати Особистий ключ у разі його компрометації;
- надавати Підприємству повну та дійсну інформацію, необхідну для формування реєстраційного запису користувача в Системі та посиленого сертифіката відкритого ключа;

– негайно інформувати Підприємство про такі події, що трапилися до закінчення строку чинності посиленого сертифіката відкритого ключа користувача, а саме:
а) компрометацію Особистого ключа;
б) виявлену неточність або зміну даних (реквізитів), а саме прізвища, місця роботи, посади, зазначених у посиленому сертифікаті відкритого ключа;
– використовувати програмне забезпечення для користування Системами тільки за призначенням в порядку, визначеному в Інструкціях з користування Системою;
– підтримувати у робочому стані програмно-технічні засоби, які необхідні для роботи програмного забезпечення для користування Системами згідно з вимогами Інструкцій з користування Системою;
– забезпечувати цілісність та незмінність програмного забезпечення для користування Системами;
– виключати можливість впливу на програмне забезпечення для користування Системами або на його роботу інших осіб або програмно-технічних засобів.

Користувачу забороняється:
– обробляти з використанням програмного забезпечення для користування Системами інформацію, що містить відомості, які становлять державну таємницю або є службовою інформацією;
– розголошувати склад інформації на власному носії ключової інформації або пароль доступу до нього, а також передавати цей носій іншим особам, виводити значення Ключів та інших ключових даних на дисплей, принтер або інші засоби візуального відображення інформації;
– повторно використовувати носії ключової інформації без попереднього знищення на них ключової інформації згідно встановленого порядку;
– використовувати носії ключової інформації у режимах, що не передбачені порядком їх штатного застосування;
– записувати на носії ключової інформації іншу інформацію окрім такої, що передбачена для функціонування програмного забезпечення для користування Системами;
– при зміні пароля доступу до носія ключової інформації або Особистого ключа вводити у якості нового значення його попереднє значення або тривіальне значення;
– застосовувати програмне забезпечення для користування Системами, які проявляють явні ознаки неправильного функціонування;
– несанкціоновано вносити зміни до програмного забезпечення для користування Системами;
– залишати власний носій ключової інформації у зчитувачі після закінчення роботи з ним;
– залишати без контролю увімкнені незаблоковані (засобами операційної системи) комп'ютери, які використовуються при функціонуванні програмного забезпечення для користування Системами, після проходження авторизації в Системі.

Користувач несе відповідальність за зберігання власного носія ключової інформації та пароля доступу до нього та Особистого ключа.

3. Порядок дій користувача при компрометації Особистих ключів та носіїв ключової інформації

У випадку компрометації Особистого ключа, носія ключової інформації або виникнення обґрунтованої підозри щодо такої компрометації користувач негайно повідомляє Підприємство та діє згідно його вказівок.

Передача даних в мережевих програмних засобах із використанням скомпрометованих Особистих ключів, або щодо компрометації яких виникли обґрунтовані підозри, забороняється.

Користувач зобов'язаний звернутися до Акредитованого центру сертифікації ключів для скасування відповідного посиленого сертифіката відкритого ключа відповідно до вимог Регламенту.

МЕН № 4 (88), серпень, 2016 р.

Додаток 2

ПАМ'ЯТКА
в разі виявлення незаконного втручання
в роботу електронно-обчислювальних машин нотаріуса

1. Самостійно або за допомогою комп'ютера зайдіть в Реєстр під своїм паролем та ключем та перевірте виконані дії «по співробітнику» за певний період, сформуйте та роздрукуйте їх.
2. Складіть лист до Державного підприємства «Національні інформаційні системи» Міністерства юстиції України, в якому вкажіть, що Вам стало відомо про несанкціоноване втручання в роботу під Вашим паролем і ключем до Державного реєстру і Ви звертаєтесь з проханням блокувати персональні (особисті) ключі, внесіть запис до книги вихідної кореспонденції та долучіть примірник до відповідного наряду. Зателефонуйте до ДП «Інформаційні системи України» та надішліть лист факсом на їх адресу, копію про підтвердження підкріпіть до цього листа.
3. Напишіть заяву до Національної поліції, в якій вкажіть, що Вам стало відомо про те, що з використанням Вашого пароля та ключа в Державному реєстрі були сформовані відповідні заяви та прийняті рішення, вкажіть номери, час та від імені кого та в інтересах кого вчинялися дії (сформуйте відповідну таблицю), та Ви звертаєтесь з проханням порушити кримінальну справу за ст. 361 Кримінального кодексу України.
4. На копії заяви про порушення кримінальної справи проставте відмітку відповідного відділення Національної поліції та внесіть запис до книги вихідної кореспонденції та долучіть примірник до відповідного наряду.
5. У поліції наполягайте на допиті Вас в якості потерпілого та отримайте пам'ятку потерпілого.
6. Повідомте про виявлені факти в телефонному режимі і надішліть листи на адресу голови Вашого відділення НПУ та Комісії НПУ з питань запобігання та протидії кіберзлочинності (секретар комісії: Elena.notariat@gmail.com).
7. По можливості визначте всі комп'ютери, з яких Вами здійснювався доступ до Реєстрів, складіть список всіх комп'ютерів, ноутбуків з яких в будь-який час здійснювався доступ до Реєстрів, як за допомогою встановленої комп'ютерної програми та і через браузер.
8. Відключіть комп'ютер від комп'ютерної мережі. У випадку, якщо в момент виявлення інциденту комп'ютер виключений, не включайте його до створення так званого «образу» жорсткого диску. Якщо комп'ютер у момент виявлення інциденту включений, зробіть наступні кроки:

– відключіть його від провідної та безпровідної Wi-Fi мережі (для провідної мережі від'єднайте сітьовий шнур, для безпровідної мережі — деактивуйте Wi-Fi адаптер);
– зафіксуйте, чи співпадає системний час комп'ютера з поточним часом (якщо ні, зафіксуйте різницю);
– виключіть комп'ютер шляхом екстреного відключення від живлення (відключення шнура від блоку живлення, зняття акумуляторної батареї).

9. Категорично заборонено виконувати антивірусні перевірки та видалення «шкідливих» програм, переустановлення операційної системи та виконувати інші дії, направлені на відновлення працездатності комп'ютера або операційної системи. Це може призвести до неможливості відновити повну картину інциденту та відновлення видалених файлів.
10. Отримайте нові ключі ЕЦП доступу до Єдиних та Державних реєстрів та замініть облікові дані особистого ключа, а також замініть паролі доступу до всіх онлайн-сервісів (пошта, соціальні мережі та інше).

11. Проаналізуйте електрону пошту, яка використовувалась на комп'ютерах, задіяних в інциденті. Спробуйте найти підозрілі листи з вкладення, які містять текст, що закликає в імперативному порядку відкрити вкладений документ або змінити настройки комп'ютера/програмного забезпечення, наприклад, включити макроси Microsoft Office.

12. Направте на адресу ДП «Національні інформаційні системи України» запит, в якому вкажіть, що просите надати інформацію, щодо того, з яких IP-адрес було здійснено реєстрацію таких заяв (№№) та просите вказати Хост (ip-адресу, ім'я комп'ютера) та ім'я користувача, з яких здійснювався вхід в реєстр під ЕЦП і логіном нотаріуса.

13. У разі наявності веб-сайту підготуйте та направте запит хостінг-провайдеру з проханням підготувати журнали відвідувань сайта за період до трьох місяців до першого інциденту.

14. Створіть образи жорстких дисків. Для цього бажано залучити незалежного технічного спеціаліста або особу, яка володіє достатнім рівнем технічних знань. Відібрані зразки необхідно оформити протоколом, який підписує нотаріус, технічний спеціаліст, по можливості адвокат та 2 особи (свідки) , які не пов'язані з роботою нотаріуса.

Носії, на яких записані копії, необхідно запакувати та опечатати. Допустимо помістити диск у поліетиленовий пакет та скріпити його ниткою на кінець, якої наклеїти пояснювальну записку з підписами осіб, які були присутні та відбирали зразки, і проставити печатку технічної організації, спеціаліст якої був присутній.

15. Замовте комп'ютерно-технічну експертизу в державній або незалежній експертній організації.

Для проведення експертизи необхідно надати запаковані носії інформації, пояснення про обставини справи, копії відповідей на запити до ДП «Інформаційні системи України», інтернет і хостинг-провайдерів, відповідну таблицю з реєстраційними діями які були вчинені від вашого імені.

Державні експертні установи

– Науково-дослідні інститути судових експертиз Міністерства юстиції України.
– Державний науко-дослідний експертно-криміналістичний центр МВС України.
– Науково-дослідний експертно-криміналістичний центр МВС України в м. Києві та областях.

Незалежні експертні організації

– ООО «Лабораторія комп'ютерної криміналістики», м. Київ, пер. Коломийський, 13/23, тел. 044-338-32-31, директор Прокопенко С.Д.

Експертизу в рамках кримінального провадження призначає слідчий Національної поліції відповідного відділення поліції, яке буде розслідувати цей злочин.

Додаток 3

ВИЯВЛЕННЯ МОЖЛИВИХ ПРОГРАМ ЗІ ШКІДЛИВИМИ ФУНКЦІЯМИ, ЯКІ БЕРУТЬ УЧАСТЬ В АТАКАХ НА НОТАРІУСІВ

У разі якщо інцидент уже виявлено, описані дії необхідно виконувати після створення образів жорсткого диска і оперативної пам'яті.

Видаляти знайдені програми і зібрані ними дані настійно не рекомендується.

Індикатори компрометації

1. Наявність в системі встановленої програми віддаленого доступу LiteManager (не плутати з SQliteManager).

2. Наявність у системі встановленої модифікованої версії програми зміни автоматичної розкладки PuntoSwitcher.

3. Наявність у системі файлу keylog.exe.

Усі наступні дії мають бути зроблені користувачем операційної системи, який має права адміністратора.

Перевірка наявності програми LiteManager

Запустити редактор реєстру: Пуск – в рядку пошуку набрати regedit – натиснути Enter.

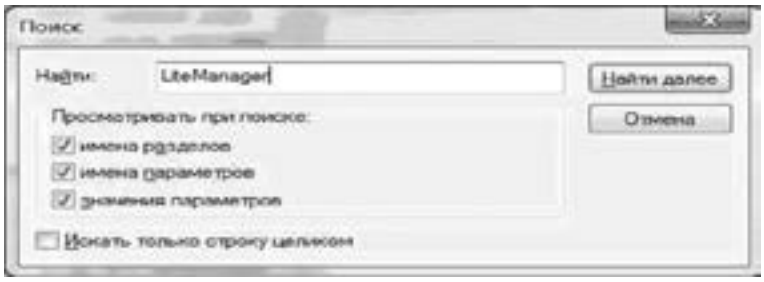
У вікні редактора реєстру перейти до розділу HKEY_CURRENT_USER\Software. Перевірити наявність розділу LiteManagerTeam.

Виконати аналогічну перевірку в розділі

HKEY_LOCAL_MACHINE\Software.

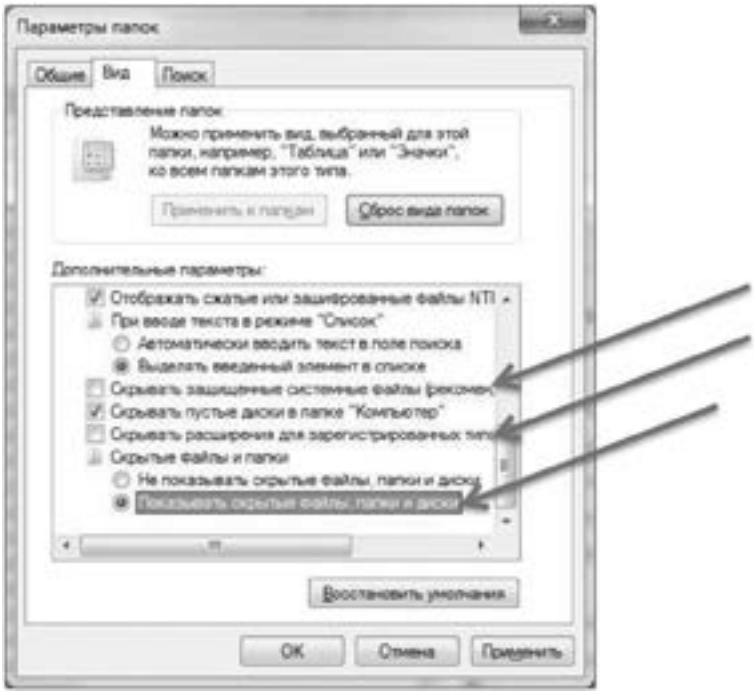
Можливо також виконати пошук за реєстром рядка LiteManager.

Для цього в меню *Правка* вибрати пункт *Знайти*, в полі ввести рядок, натиснути З*найти далі*:



Включити відображення прихованих і системних файлів. Для цього *Пуск – Панель управління – властивості папки*.

На вкладці *Вид* зняти галочки біля опцій «Приховувати захищені системні файли» і «Приховувати розширення для зареєстрованих типів файлів», переключити опцію «Показувати приховані файли, папки і диски», натиснути «Застосувати», «ОК».



Запустити Провідник або інший файловий менеджер.

Перейти по шляху C:\Users\Ім'я користувача\AppData\Roaming\.

Перевірити наявність папки **ServiceUpdate, Windows32** (або зі схожим ім'ям), в якій містяться файли System_32.exe, Config.xml. (в одній папці мають міститись обидва файли).

Можна також виконати пошук за диском C:\ файлів з зазначеними іменами System_32.exe, Config.xml.

Увага! *Файл config.xml може міститись в інших папках і відноситись до звичайних програм, і цей файл самостійно не може бути шкідливим.*

Наприклад, результат пошуку, в якому знайдено файл, але він відноситься до інших програм та не є шкідливим.

МЕН № 4 (88), серпень, 2016 р.

Перевірка наявності програми PuntoSwitcher

Запустити редактор реєстру: Пуск – в рядку пошуку набрати regedit – натиснути Enter.

У вікні редактора реєстру перейти до розділу

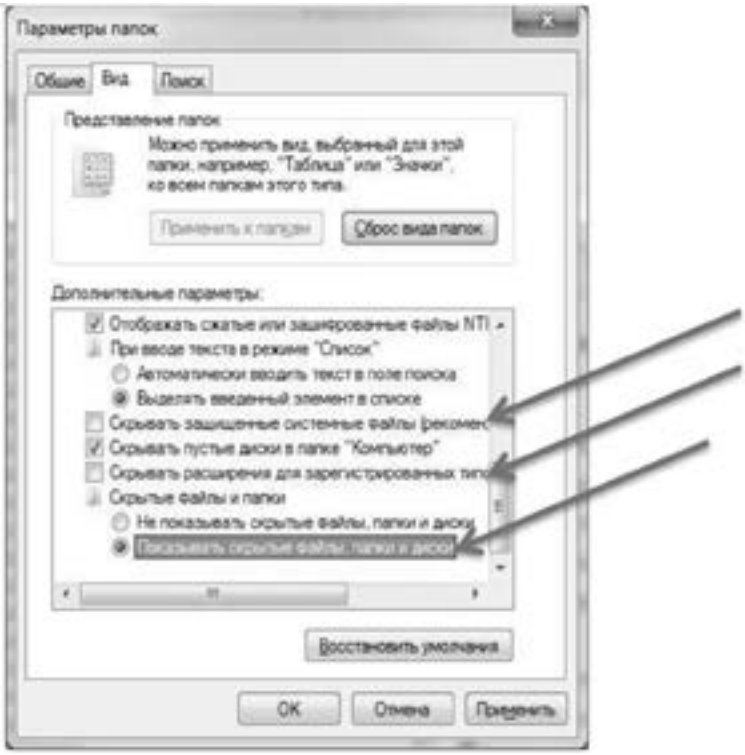
HKEY_CURRENT_USER\Software\AppDataLow\Yandex\Yupdate-BITSCM\Applications\. Перевірити наявність розділу Punto.

Можливо також виконати пошук за реєстром рядка Punto.

Для цього в меню *Правка* вибрати пункт *Знайти*, в полі ввести рядок Punto, натисніть кнопку *Знайти далі*.

Включити відображення прихованих і системних файлів.

Для цього *Пуск – Панель управління – властивості папки*.



На вкладці *Вид* зняти галочки біля опцій «Приховувати захищені системні файли» і «Приховувати розширення для зареєстрованих типів файлів», переключити опцію «Показувати приховані файли, папки і диски», натиснути «Застосувати», «ОК».

Запустити Провідник або інший файловий менеджер.

Перейти по дорозі C:\Users\Ім'я користувача\AppData\Roaming\.

Перевірити наявність папки Windows, в якій містяться файли windows.exe, diary.exe, ps64ldr.exe, pshook.dll.

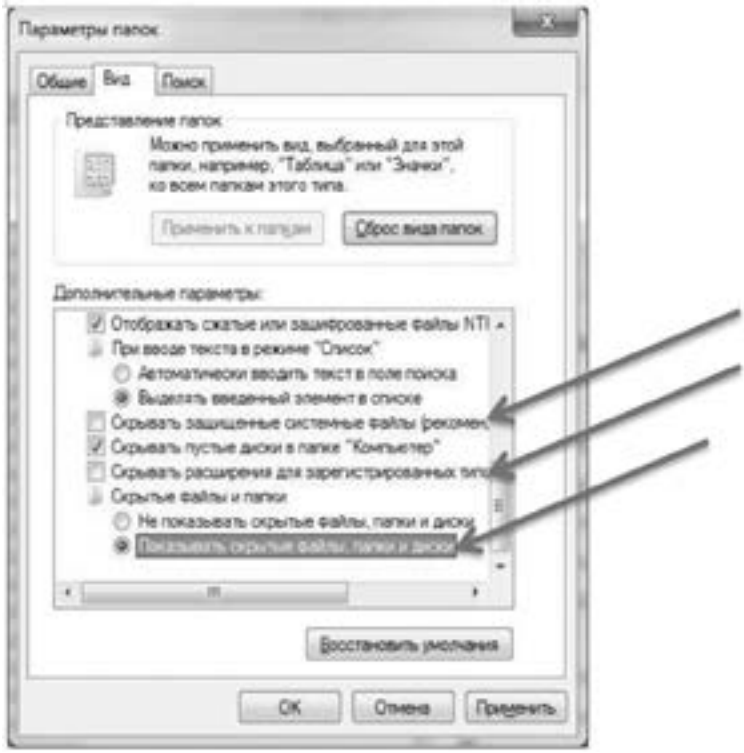
Можна також виконати пошук за диском C: файлів з зазначеними іменами windows.exe, diary.exe, ps64ldr.exe, pshook.dll.

Увага! *Файл windows.exe не обов'язково є шкідливим і необхідно аналізувати ситуацію в цілому, а також перевіряти наявність інших зазначених файлів.*

Перевірка наявності файлу keylog.exe

Включити відображення прихованих і системних файлів.

Для цього *Пуск – Панель управління – властивості папки*.



На вкладці *Вид* зняти галочки біля опцій «Приховувати захищені системні файли» і «Приховувати розширення для зареєстрованих типів файлів», переключити опцію «Показувати приховані файли, папки і диски», натиснути «Застосувати», «ОК».

Виконати пошук за всіма локальними дисками файлів за іменем keylog.exe.

Додаток 4

РЕКОМЕНДАЦІЯ ЩОДО ЗМІЦНЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НОТАРІАЛЬНОГО ОФІСУ

Ця рекомендація визначає кроки для підтримання належного рівня інформаційної безпеки нотаріального офісу з метою запобігання перехоплення третіми особами через Інтернет інформації, що становить нотаріальну таємницю, а також ідентифікаторів доступу до Єдиних та Державних реєстрів.

Основні дії, які мають бути вчинені нотаріусом (ці дії можна вчиняти періодично)

1. Змініть усі паролі, у тому числі встановлені за замовчуванням, які зараз вами використовуються на комп'ютерах нотаріального офісу (пароль входу в операційну систему комп'ютерів, пароль входу до електронних поштових скриньок, пароль ключа ЕЦП, пароль входу до реєстрів, пароль доступу до мережі Wi-fi) (далі — інформаційна система):

а) змініть паролі за замовчуванням, а також встановіть пароль входу в операційну систему, якщо такий відсутній;

б) використовуйте різні паролі для різних облікових записів та різних комп'ютерів;

в) використовуйте складні паролі для додаткової безпеки (використовуйте великі та маленькі літери, цифри, інші символи).

2. Заблокуйте доступ до вашої локальної мережі або мережі Wi-fi:

а) доступ до локальної мережі можуть мати лише виключно комп'ютери та техніка Вашої мережі;

б) якщо ви використовуєте мережу Wi-fi, то до неї можуть мати доступ виключно комп'ютери та техніка Вашої мережі;

МЕН № 4 (88), серпень, 2016 р.

в) якщо Вашим клієнтам необхідний доступ до Інтернету або до принтера, надайте цей доступ через окрему (гостьову) мережу Wi-fi або безпосередньо під'єднайте принтер до ноутбука клієнта.

3. Використовуйте останні версії програмного забезпечення (ПЗ), патчі, оновлення:

а) виробники ПЗ постійно випускають оновлення для виправлення відомих вразливостей. Тримайте операційну систему, офісну програму, антивірусну-антишпигунську програму в актуальному стані (оновлену), щоб запобігти нападникам (кіберзлочинцям) здійснювати протиправні дії — втручання у Вашу інформаційну мережу за допомогою використання таких вразливостей.

4. Відключіть в операційній системі функцію віддаленого доступу, а також вимкніть автоматичне завантаження сторонніх програм, що дозволяють віддалене управління комп'ютером.

Деякі операційні системи та сторонні програми, надають функціонал для віддаленого моніторингу Вашого комп'ютера, у тому числі веб-сторінку.

5. Виключіть мікрофон, коли він не використовується.

Приглушений мікрофон буде перешкоджати несанкціонованому прослуховуванню приміщення третіми особами.

6. Відключіть веб-камеру, коли вона не використовується:

а) направте камеру у напрямку стіни або в інше місце, що буде перешкоджати несанкціонованому її перегляду третіми особами;

б) закрита лінза (об'єктив) камери буде перешкоджати несанкціонованому її перегляду третіми особами.

7. Встановіть періодичність обов'язкової зміни паролів доступу до елементів Вашої інформаційної системи та її перевірку:

а) періодично змінюйте всі паролі доступу до елементів інформаційної системи;

б) періодична зміна паролів не дасть зловмиснику додатковий час для їх підбору та використання;

в) періодично здійснюйте перевірку Ваших комп'ютерів за допомогою антивірусних-антишпигунських програм;

г) отримані за допомогою електронної пошти файли перед відкриттям перевіряйте за допомогою встановленої антивірусної-антишпигунської програми, а також використовуйте безкоштовний веб-сервіс https://www.virustotal.com/, що здійснює дослідження підозрілих файлів і посилань; дозволяє швидко виявляти віруси, хробаки, трояни й інші види шкідливих програм.

8. Відключайте мережу Wi-fi, комп'ютери, запущені реєстри, коли вони не використовуються:

а) вимкнення Wi-fi, комп'ютерів, коли вони не використовуються, обмежуватиме кількість часу, коли атакуючі можуть спробувати отримати доступ до Вашої інформаційної системи з мережі Інтернет;

б) закривайте програми Єдиних та Державних реєстрів, коли не використовуєте їх, не залишайте комп'ютери без нагляду з увімкненими програмами реєстрів.

9. Унеможливіть фізичний доступ третіх осіб до комп'ютерів Вашого офісу та конфіденційної інформації:

а) за можливості не використовуйте сторонні носії інформації (флешки, карти пам'яті, диски тощо) на комп'ютерах Вашого офісу;

б) перед використанням носія інформації обов'язково здійсніть його перевірку за допомогою антивірусної-антишпигунської програми;

в) перед обслуговуванням сторонніми особами Ваших комп'ютерів вийміть усі носії інформації, що містять конфіденційні дані, ключі ЕЦП;

г) не залишайте носії інформації з ключами ЕПЦ у комп'ютерах, коли їх не використовуєте.

10. Використання безкоштовних сервісів електронної пошти:
а) використовуйте поштові сервіси відомих безпечних провайдерів послуг;
б) не використовуйте поштові сервіси країн-агресорів по відношенню до України;
в) використовуйте поштові сервіси, що надають захист від вірусів, шпигунів тощо;
г) використовуйте поштові сервіси, що надають змогу переглядати прикріплені файли не завантажуючи їх;
ґ) використовуйте поштові сервіси, що використовують при вході дворівневу аунтифікацію.

Додаток 5

КОРОТКО ПРО ГОЛОВНЕ

1. Зберігайте паролі та ключі в недоступному для сторонніх осіб місці.
2. Ніколи не залишайте фахівця з налаштування комп'ютерної техніки сам на сам з комп'ютером, на якому встановлені реєстри, та не давайте йому паролі та ключі.
3. Не розголошуйте паролі від мережі WI-FI.
4. Якомога частіше змінюйте паролі доступу до реєстрів з використанням складних комбінацій.
5. Не відкривайте електронні листи з невідомих Вам адресатів і негайно видаляйте їх.
6. Не відкривайте файли клієнтів з їх флеш-носіїв.

При підготовці Методичних рекомендацій використано матеріали

1. Приватного нотаріуса Київського міського нотаріального округу Козаєвої Н.М.
2. Приватного нотаріуса Київського міського нотаріального округу Солошенка А.В.
3. Приватного нотаріуса Київського міського нотаріального округу Донченко О.О.
4. Головного територіального управління юстиції у Рівненської області.
5. Відділення НПУ в Рівненській області.
6. Приватного нотаріуса Херсонського міського нотаріального округу Сперчуна О.О.
7. Приватного нотаріуса Сейдалієва Д.С.
8. ТОВ «Лабораторія комп'ютерної криміналістики» CeberLab.