УДК 34.037

Храпенко В. С.,
аспірант кафедри адміністративного і кримінального права
юридичного факультету
Дніпровського національного університету імені Олеся Гончара

ПРОТИДІЯ НОТАРІУСІВ КІБЕРЗЛОЧИНАМ, ЩО ВЧИНЯЮТЬСЯ В ПРОЦЕСІ ДЕРЖАВНОЇ РЕЄСТРАЦІЇ ПРАВ НА НЕРУХОМЕ МАЙНО

THE CONTERACTION OF NOTARIES TO THE CYBERCRIMES THAT ARE COMITTED IN THE PROCESS OF STATE REGISTRATION OF RIGHTS TO REAL ESTATE

У статті розглянуто проблеми інформаційної безпеки та незаконного доступу до закритих даних, що виникають під час здійснення нотаріусами функцій державного реєстратора.

Ключові слова: *нотаріус, кіберзлочин, державна реєстрація прав, несанкціонований доступ.*

В статье рассмотрены проблемы информационной безопасности и незаконного доступа к закрытым данным, которые возникают при осуществлении нотариусами функций государственного регистратора.

Ключевые слова: *нотариус, киберпреступление, государственная регистрация прав, несанкционированный доступ.*

The problems of information security and Illegal access to private data that raised when notaries perform functions of state registrars, are considered in the article.

Key words: *notary, cybercrime, state registration of rights, unauthorized access.*

З набранням чинності Закону України «Про внесення змін до деяких законодавчих актів України щодо вдосконалення та спрощення процедури державної реєстрації земельних ділянок та речових прав на нерухоме майно» від 04.07.2012 р. № 5037-VI, в нашій державі почала діяти нова система реєстрації речових прав на нерухоме майно та їх обтяжень. Її введення у практику стало результатом комплексної реформи у сфері реєстрації речових прав на нерухомість та їх обтяжень, що була запроваджена урядом із метою адаптації вказаної системи до стандартів Європейського Союзу [1]. Одним із нововведень реформи стало отримання нотаріусами повноважень щодо проведення реєстрації права власності, користування нерухомим майном, усіх інших речових прав і їх обтяжень безпосередньо під час вчинення нотаріальної дії [2].

Як зазначає М.М. Дякович, з 1 січня 2013 р. законодавством було встановлено нові підходи щодо реєстрації речових прав, сформовано реєстраційні органи таким чином, що часткове передання функцій із реєстрації речових прав та їх обтяжень нотаріусам усунуло бюрократичні перешкоди в процедурі реєстрації, ліквідувало часову прогалину між укладенням договору, його нотаріальним посвідченням і виникненням права власності [3, с. 75].

З 1 січня 2016 р., у зв'язку з прийняттям відповідних змін до законодавства, нотаріусів було наділено ще більш широкими повноваженнями, а саме повноваженнями державних реєстраторів прав на нерухоме майно, відповідно до яких вони можуть здійснювати державну реєстрацію речових прав на нерухоме майно та їх обтяжень і без вчинення нотаріальної дії щодо такого майна [4].

Окремі аспекти реформованого інституту державної реєстрації речових прав на нерухоме майно та їх обтяжень висвітлюються у працях таких вчених, як-от: Г.С. Дьомкіна, М.М. Дякович, Т.В. Лісова, С.В. Нечипорук, О.В. Степська, К.І. Чижмарь. Проте загрозам інформаційної незахищеності, що виникають у цій сфері, з огляду на розвиток комп'ютерних технологій, увага не приділялася.

На сьогодні усі дані про реєстрацію будь-якої нерухомості вносяться до електронного реєстру, для доступу до якого нотаріус використовує свій унікальний код (так званий ключ) та електронний цифровий підпис, які знаходяться на комп'ютері нотаріуса або зберігаються на флеш-карті. Вищезазначені нововведення, а також запроваджений принцип екстериторіальності сприяли спрощенню процедури державної реєстрації речових прав на нерухоме майно [5]. Однак, крім явних переваг, швидкі зміни у законодавстві актуалізували низку ризиків, які одразу ж проявилися у нотаріальній практиці.

Так, за наявною у Нотаріальної палати України інформацією, лише в період з квітня 2015 р. по травень 2016 р. було вчинено близько 300 сторонніх втручань у роботу Державного реєстру речових прав, у результаті яких було здійснено неправомірні дії, пов'язані з припиненням обтяжень та іпотек, зняттям арештів та подальшої незаконної перереєстрації права власності.

Внаслідок сторонніх втручань постраждало понад двадцять українських нотаріусів із різних областей. Через специфіку роботи правоохоронних органів подібні втручання призводили до настання вкрай несприятливих для нотаріусів наслідків, що полягали, насамперед, у відмові порушувати кримінальне провадження за заявою нотаріусів про вчинення кібератаки на робочий комп'ютер. Проте навіть порушення кримінальної справи не завжди сприяє звільненню нотаріусів від відповідальності

за сторонні втручання в роботу реєстрів від їх імені. Так, дії нотаріуса Житомирського міського нотаріального округу було визнано Вищим спеціалізованим адміністративним судом протиправними, незважаючи на визнання цього нотаріуса потерпілим у відповідному кримінальному провадженні. Нотаріуси в подібних випадках, відповідно, змушені витрачати власний час та кошти для участі в судових засіданнях і самостійно доводити свою невинуватість.

Збільшення кількості кібератак змусило нотаріусів порушити питання протидії кіберзлочинам у сфері державної реєстрації прав на Позачерговому з'їзді нотаріусів України, що проходив у місті Києві 22–23 квітня 2016 р. На з'їзді було відмічено, що проведення незаконних реєстраційних дій відбувається зазвичай у період відпусток нотаріусів, що є державними реєстраторами, у вихідні та святкові дні, вечірній та нічний час. Відповідно до висновку, наданого ТОВ «Лабораторія комп'ютерної криміналістики» CyberLab, здебільшого на обрані для хакерської атаки комп'ютери встановлювалося шкідливе програмне забезпечення LiteManager, яке давало змогу хакерам віддалено керувати комп'ютером та викрадати дані облікових записів, причому шкідливий файл надходив до нотаріусів у вигляді вкладення в повідомлення електронної пошти, що надсилалися нібито від імені Міністерства юстиції України.

У результаті обговорень, проведених на з'їзді, було вирішено звернутися до Міністерства юстиції України з приводу розроблення комплексу заходів з метою підвищення ступенів захисту інформації, що міститься в Єдиних та Державних реєстрах, модернізації програмного забезпечення Державного реєстру речових прав, забезпечення співпраці Державного підприємства «Національні інформаційні системи» як технічного адміністратора реєстру із провідними фахівцями в галузі боротьби з кіберзлочинністю. Однак основним досягненням проведення з'їзду стало покладення початку створення постійно діючого робочого органу Нотаріальної палати України – Комісії з питань запобігання та протидії кіберзлочинності. Відповідне рішення було затверджене Резолюцією Позачергового з'їзду нотаріусів України від 22–23 квітня 2016 р. з приводу низки сторонніх втручань до Державного реєстру речових прав (ДРРП) шляхом використання логіну, пароля, ключа ЕЦП нотаріуса та заходів протидії кіберзлочинам у сфері державної реєстрації прав [6].

Завдання створення комісії було покладено на Президента та Раду Нотаріальної палати України. Результатом їх роботи стало затвердження протоколом № 30 Ради Нотаріальної палати України від 31 травня 2016 р. Положення про комісію з питань запобігання та протидії кіберзлочинності [7]. Основними функціями, якими було наділено Комісію, стали розробка та надання пропозицій щодо запобігання, виявлення та припинення кіберзлочинних діянь, організація та проведення профілактичної роботи серед нотаріусів України з метою попередження несанкціонованих втручань до реєстрів, взаємодія з державним та правоохоронними органами України щодо обміну інформацією, планування та проведення спільних заходів у сфері протидії кіберзлочинності.

7 червня 2016 р. відбулося перше організаційне засідання Комісії Нотаріальної палати України з питань запобігання та протидії кіберзлочинності. Окрім обрання керівного складу та вирішення суто організаційних питань, було напрацьовано певні механізми реагування на спроби несанкціонованого втручання в роботу реєстрів. Одним із таких механізмів стала процедура верифікації, додаткового захисту та опрацювання технології перевірки комп'ютерного обладнання, яке використовується нотаріусами під час здійснення професійної діяльності [8].

Одним із перших напрацювань новоствореної комісії стала розробка Методичних рекомендацій щодо підтримання належного рівня інформаційної безпеки нотаріального офісу [9], головною метою яких є запобігання перехоплення третіми особами через мережу Інтернет інформації, що містить нотаріальну таємницю, та ідентифікаторів доступу до Єдиних та Державних реєстрів. Розробники рекомендацій нагадали нотаріусам, що значну роль у полегшенні доступу зловмисників до закритих даних відіграє, як правило, не технічний, а людський фактор. Було відзначено найбільш розповсюджені помилки нотаріусів у роботі з реєстрами, які дають змогу кіберзлочинцям отримувати конфіденційну інформацію. Як виявилося, нотаріуси досить часто копіюють електронні ключі, надані їм для доступу до реєстрів, на кілька флеш-носіїв, заходять у реєстри з кількох комп'ютерів, дозволяють користуватися своїми особистими ключами помічникам та довіреним особам, що, безперечно, збільшує вірогідність доступу до таких ключів зловмисників.

Також нотаріуси нехтують встановленням на своєму робочому комп'ютері антивірусних програм, під'єднують робочий комп'ютер до загальнодоступної мережі Wi-Fi, зберігають паролі доступу до реєстрів у вигляді файлів Microsoft Office Word, розміщуючи їх на робочому столі, що призводить до копіювання таких файлів сторонніми особами без особливих зусиль.

Перераховані шляхи втрати нотаріусом конфіденційних даних дають змогу зловмисникам швидко та легко отримувати дані для реалізації своїх незаконних намірів.

Проте існують і більш досконалі методи, які хакери використовують для злому паролів нотаріусів. Загалом дані методи можна поділити на дві групи.

До першої групи належать методи, що полягають у підбиранні пароля хакером особисто. Сюди входять: підбирання пароля за допомогою файлу, що містить словник із найбільш розповсюджених слів, які можуть використовуватися нотаріусами; підбирання пароля методом перебору всіх можливих комбінацій букв та цифр; підбирання пароля з використанням інформації про жертву, зібраної в мережі Інтернет (наприклад, на сторінці у соціальній мережі

можуть бути перераховані хобі, захоплення, прізвиська домашніх тварин, дата народження близьких родичів жертви, які вона, ймовірно, використовує як пароль); використання райдужної таблиці, що включає в себе числові значення всіх можливих комбінацій зашифрованих паролів для будь-якого алгоритму шифрування.

Друга група методів використовується хакерами для того, щоб нотаріус особисто повідомив їм свій пароль, сам того не підозрюючи. До них належать:

1) фішинг – метод, що полягає у розсиланні повідомлень із проханням повідомити особисті дані. У такому разі хакер маскується під адміністратора сайту онлайн-банкінгу, електронної платіжної системи або іншого інтернет-ресурсу, яким користується нотаріус в процесі своєї повсякденної діяльності;

2) соціальна інженерія – аналогічний фішингу метод, що використовується у реальному світі, а не за допомогою поштової скриньки. Зловмисник, наприклад, може зателефонувати до нотаріального офісу під видом співробітника IT-безпеки та попросити пароль доступу до мережі;

3) метод підглядання, що може бути використаний найбільш самовпевненими злочинцями, які, проникаючи до нотаріального офісу під видом кур'єра, фахівця з технічного обслуговування або іншої особи, крадуть паролі, що містяться, наприклад, на стікерах, наклеєних на монітор, нотатках на робочому столі, або ж особисто вводяться нотаріусом в їх присутності;

4) використання шкідливого програмного забезпечення, яке дає змогу зчитувати інформацію, зокрема й конфіденційну, безпосередньо з клавіатури (так званий кейлоггер), або створює скріншоти під час процесу авторизації, або шукає на комп'ютері файл із паролями веб-браузера інтернет-користувача та надсилає його на адресу злочинця.

Варто зазначити, що вищенаведені способи хакерських атак постійно вдосконалюються та поповнюються новими. Стрімкий розвиток інформаційних технологій потребує від Комісії НПУ із запобігання та протидії кіберзлочинності швидкого реагування, вивчення нових схем незаконного втручання в роботу реєстрів, розроблення заходів щодо їх відвернення та регулярного оновлення Методичних рекомендацій для своєчасного інформування нотаріусів про появу нових загроз.

Іншою важливою інформацією для нотаріусів, яка наразі викладена у Методичних рекомендаціях щодо підтримання належного рівня інформаційної безпеки нотаріального офісу, є список найбільш розповсюджених ознак можливого злому комп'ютера або його зараження шкідливими програмами. До таких ознак Комісія відносить: істотне уповільнення роботи комп'ютера, неможливість видалення деяких файлів або їх самокопіювання після видалення, повне або часткове блокування системних функцій комп'ютера, втрата даних, що зберігаються на жорсткому диску, підозріло високий вихідний інтернет-трафік, поява підозрілих файлів у кореневих директоріях жорсткого диску або ж найбільш очевидна ознака зараження комп'ютера вірусом – повідомлення антивірусного захисту про присутність на комп'ютері троянських програм. Останні, хоч і дедалі рідше використовуються хакерами через свою простоту та застарілість, проте продовжують залишатися надійним та ефективним способом отримати повний контроль над зараженим комп'ютером.

Найбільш дієвими заходами, які необхідно здійснювати нотаріусам для забезпечення безпеки свого робочого комп'ютера та попередження несанкціонованого доступу до особистих даних, Комісією у Методичних рекомендаціях запропоновано збереження антивірусної програми та файрволу у постійно ввімкненому та оновленому стані, використання лише останніх версій програмного забезпечення комп'ютера; створення додаткового облікового запису спеціально для роботи з реєстрами, блокування екрану комп'ютера перед відлученням від робочого місця; періодичну зміну паролів користувачів на комп'ютерах, використання якомога складніших паролів, довжиною не менш ніж дванадцять символів, які не містять особистих даних користувача; попередній перегляд вмісту листів, що надходять на електронну пошту, за допомогою антивірусного сервісу virustotal; користування, за можливості, лише сайтами, які застосовують шифрування вхідної та вихідної інформації.

Усі перераховані вище рекомендації Комісії було взято нотаріусами України на озброєння, однак, незважаючи на це, повністю уникнути кібератак їм так і не вдалося. Напередодні новорічних та різдвяних свят, з 21 по 24 грудня 2016 р. Комісією було зафіксовано посилення активності зловмисників. За цей короткий період відбулося 18 вторгнень в інформаційний простір нотаріальних офісів шляхом розсилання шкідливої програми на електронні адреси нотаріусів. Від імені одного з нотаріусів зловмисниками розсилався електронний лист, який містив у собі вірусний файл, що під час відкриття копіював конфіденційні дані з флеш-носіїв та робочих комп'ютерів. Адреса, з якої надсилався лист, могла змінюватися, що ускладнювало ідентифікацію нотаріусами отриманого листа як потенційно шкідливого.

Через це до голів відділень нотаріальної палати України з терміновим листом звернулася голова Комісії Н.М. Козаєва [10]. У зверненні вона зазначила, що у разі виникнення аналогічних ситуацій нотаріусам необхідно своєчасно перевіряти пошту та діяти чітко за інструкцією, що розроблена Комісією з метою запобігання викрадення зловмисниками секретних даних у майбутньому. У інструкції було запропоновано перед видаленням підозрілого файлу заповнювати форму встановленого зразка задля того, щоб подібні файли легше було виявляти у майбутньому, а у разі, якщо шкідливий файл все ж таки було завантажено на комп'ютер, – встановлювати зазначений в інструкції антивірус та здійснювати з його допомогою повну перевірку робочого комп'ютера, попередньо від'єднавшись від мережі

Інтернет. Файл вірусу, з допомогою якого було атаковано робочі комп'ютери нотаріусів наприкінці грудня 2016 р., було передано Комісією до компанії ESET NOD32 Україна задля його класифікації та блокування у майбутньому.

Одним із напрацювань, що вдалося здійснити до кінця 2016 р. у рамках роботи Комісії з питань запобігання та протидії кіберзлочинності, стало узгодження функціонування Єдиних та Державних реєстрів з новими вимогами законодавства щодо використання нотаріусами захищених носіїв ключової інформації електронного цифрового підпису (ЕЦП). Відповідні зміни були внесені в Закон України «Про електронний цифровий підпис» 06 жовтня 2016 р. [11]. Результатом спільної роботи Комісії з Державним підприємством «Національні інформаційні системи» та підприємством-розробником засобів криптографічного захисту інформації – приватним акціонерним товариством «Інститут інформаційних технологій» – стало переведення програмного забезпечення реєстрів у період до 1 квітня 2017 р. в режим роботи з підтримкою виключно захищених носіїв ключової інформації [12]. За словами розробника, перевагою захищеного носія є неможливість копіювання логіну та пароля доступу нотаріуса з віддаленого комп'ютера зловмисником, що є додатковим заходом посилення інформаційної безпеки нотаріусів України.

Тривалий час право доступу до Єдиних та державних реєстрів Міністерства юстиції України мало досить вузьке коло осіб (приватні та державні нотаріуси та працівники Держінформ'юсту). Будь-який вхід користувача-нотаріуса до реєстрів контролювався інженерами Держінформ'юсту, виконані реєстраційні дії перевірялись відповідними спеціалістами, надавались поточні консультації, коригувалась практика роботи нотаріусів із реєстрами.

Останнім часом держава взяла курс на відкритість відомостей з Єдиних та державних реєстрів, а також суттєво розширила коло осіб-реєстраторів (центри надання адміністративних послуг, органи місцевого самоврядування, банки). Штат працівників ДП «НАІС» (колишній Держінформ'юст) з контролю за діями реєстраторів не змінився. Таким чином, можливість кваліфікованого контролю за правильністю та законністю дій кожного реєстратора втрачена. Отже, постає питання додаткового захисту відомостей реєстрів від стороннього несанкціонованого злочинного втручання з метою викривлення даних (зняття обтяжень/арештів щодо нерухомого майна тощо).

Відсутність надійного захисту доступу до реєстрів ставить під удар не лише авторитет нотаріуса, а й авторитет держави щодо спроможності забезпечити достатній захист програмного забезпечення Єдиного та Державного реєстрів, а отже, цілковиту законність цивільного обороту нерухомості в Україні. На сьогодні перед Комісією Нотаріальної палати України з питань запобігання та протидії кіберзлочинності стоїть ще багато завдань, що потребують невідкладного вирішення у найближчому майбутньому.

ЛІТЕРАТУРА:

1. Кочергіна Н. Нова система реєстрації речових прав на нерухоме майно та їх обтяжень [Електронний ресурс]. – Режим доступу : http://pravotoday.in.ua/ua/press-centre/publications/pub-886.

2. Коротюк О. Виконання нотаріусом функцій державного реєстратора речових прав на нерухоме майно. [Електронний ресурс]. – Режим доступу : http://korotyuk.com/vykonannya-notariusom-funktsiy-derzhavnoho-reyestratora-rechovykh-prav-na-nerukhome-mayno.html.

3. Дякович М. Нотаріус як державний реєстратор прав на нерухоме майно за законодавством України / М. Дякович // Бюлетень Міністерства юстиції України. – 2014. – № 7. – С. 73–77 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/bmju_2014_7_25.

4. З 1 січня 2016 р. набирають чинності зміни до Закону «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» [Електронний ресурс]. – Режим доступу : https://minjust.gov.ua/ ua/news/47969.

5. На допомогу рейдерам: невдачі реформи міністра Петренка [Електронний ресурс]. – Режим доступу : http://ua1.com.ua/publications/na-dopomogu-reyderam-nevdachi-reformi-ministra-petrenko-18313.html.

6. Резолюція Позачергового з'їзду нотаріусів України від 22–23 квітня 2016 р. з приводу низки сторонніх втручань до ДРРП шляхом використання логіну, пароля, ключа ЕЦП нотаріуса та заходів протидії кіберзлочинам у сфері державної реєстрації прав [Електронний ресурс]. – Режим доступу : http://vinnotariat.com.ua/teoriya-praktika/rezoluciya_23052016.pdf.

7. Положення про комісію Нотаріальної палати України з питань запобігання та протидії кіберзлочинності [Електронний ресурс]. – Режим доступу : http://old.npu.in.ua/images/Komisii/kiber/polojenya_kiber_vid_31052016.pdf.

8. Прес-реліз засідання комісії Нотаріальної палати України з питань запобігання та протидії кіберзлочинності [Електронний ресурс]. – Режим доступу : http://old.npu.in.ua/ua/novini/podiji/1429-do-uvagi-notariusiv-07062016#.WNFCPNKLS70.

9. Методичні рекомендації щодо підтримання належного рівня інформаційної безпеки нотаріального офісу [Електронний ресурс]. – Режим доступу : http://notariat.kr.ua/index/metodichka.html.

10. Лист Голови Комісії з кібербезпеки НПУ Козаєвої Н. щодо хакерських атак [Електронний ресурс]. – Режим доступу : http://unp-rivne.com/index.html?id=1400.

11. Про електронний цифровий підпис : Закон України від 22.05.2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.

12. Результати роботи НПУ щодо захищених носіїв ключової інформації електронного цифрового підпису [Електронний ресурс]. – Режим доступу : http://unp-rivne.com/index.html?id=1401.