5. Національний стандарт № 2 «Оцінка нерухомого майна», затверджений постановою Кабінету Міністрів України № 1442 від 28 жовтня 2004 року.

6. Методика експертної грошової оцінки земельних ділянок, затверджена постановою Кабінету Міністрів України № 1531 від 11 жовтня 2002 року.

7. Оцінка та управління нерухомістю: навчальний посібник / [В. Р. Кучеренко, М. А. Заєць, О. В. Захарченко, Н. В. Сментина, В. О. Улибіна]. – Одеса: Видавництво ТОВ «Лерадрук», 2013. – 272 с.

8. Порядок оцінки орендованого нерухомого майна, що містить невід'ємні поліпшення, здійснені за час його оренди, під час приватизації, затверджений наказом Фонду державного майна № 377 від 27 лютого 2004 року.

9. Цивільний кодекс України № 435-IV від 16 січня 2003 року.

10. Господарський кодекс України № 436-IV від 16 січня 2003 року.

11. Національне положення (стандарт) бухгалтерського обліку 1 «Загальні вимоги до складання фінансової звітності», затверджене наказом Міністерства фінансів України № 73 від 07 лютого 2013 року.

12. Порядок взаємодії органів державної контрольно-ревізійної служби, органів прокуратури. Внутрішніх справ, Служби безпеки України, затверджений наказом Головного контрольно – ревізійного управління України, Міністерства внутрішніх справ України, Служби безпеки України, Генеральної прокуратури України № 346/1025/685/53 від 19 жовтня 2006 року.

ДЕЯКІ ПИТАННЯ ЗАХИСТУ ПРАВА ВІЙСЬКОВОСЛУЖБОВЦІВ ТА ЧЛЕНІВ ЇХ СІМЕЙ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Бурчак Леся,
аспірант Інституту інформації, безпеки і права
Національної академії правових наук України
https://orcid.org/0009-0004-5116-4694

Аналізуючи сучасні напрями розвитку судової експертизи та криміналістики слід зазначити, що нині в криміналістичній науці майже не розроблено рекомендацій, які стосувалися б особливостей розслідування та проведення судових експертиз за категоріями справ, які стосуються комп'ютерних технологій, інтернет ресурсів і захисту персональних даних. Пов'язано це насамперед з новизною проблеми,

доступністю та стрімким збільшенням кількості різновидів комп'ютерних програм, технічного обладнання та доступу до нових технологій. Разом з тим, експертна оцінка а також захист персональних даних під час проведення експертиз має бути на належному рівні. На практиці вказаний захист персональних даних не завжди забезпечується належними чином з об'єктивних обставин, які не залежать від експерта.

З 18 травня 2024 року запрацював Єдиний електронний реєстр «Оберіг» – електронна база даних про військовозобов'язаних, призовників і резервістів, покликана спростити ведення військового обліку. «Оберіг» наповнюється автоматично інформацією з різних державних реєстрів, а також даними, зібраними працівниками ТЦК та СП. Реєстр містить персональні дані людині такі як: ім'я та прізвище, дата народження, сімейний стан, місце проживання, звання, присвоєна ВОС, відомості про освіту, судимість місце роботи, членів сім'ї, реєстраційний номер картки платника податку. Доступ до реєстру для громадян можливий через мобільний застосунок «Дія».

«Оберіг» взаємодіє з іншими державними реєстрами. Зокрема, нині із шістьма: реєстром Державної податкової служби; реєстром Державної реєстрації актів цивільного стану; реєстром Державної судової адміністрації; реєстром Державної прикордонної служби; реєстром Міносвіти; реєстром Державної міграційної служби. Також відбувається взаємодія з Міністерством цифрової трансформації та під'єднання реєстру Пенсійного фонду.

На початку липня 2024 року стався масштабний збій в системі «Оберіг». По причині цього збою військовим усіх частин максимально обмежили пересування між містами та областями та скасували відрядження, залишаючи максимально людей у розташуванні. За інформацією опублікованою в кількох медіа була надана неофіційна заборона переведення військовослужбовців з одного підрозділу в інший, щоб упродовж липня максимально оцінити кількість людей, доукомплектувати за рахунок певних підрозділів бойові частини та не допустити відтоку бойових солдатів і офіцерів із фронту.

Єдиний електронний реєстр «Оберіг» модернізували за підтримки Європейського Союзу в межах проєкту EU4DigitalUA, що впроваджує естонська Академія електронного управління. Власником реєстру та персональних даних є міністерство оборони, а розпорядник – Генеральний штаб ЗСУ. Адміністраторами реєстру визначені обласні ТЦК, а наповнення даних покладено на районні та міські центри комплектування. Доступ до даних має також СБУ та СЗРУ.

Одночасно з Єдиним електронним реєстром «Оберіг» запрацював мобільний застосунок «Резерв+». У цьому додатку

військовозобов'язані, призовники та резервісти можуть оновити свої персональні дані відповідно до Закону України «Про мобілізаційну підготовку та мобілізацію». Лише через 10 годин після запуску вказаного застосунку в ньому стався масштабний збій, який імовірно, був викликаний одночасними входами в застосунок у великій кількості збою невідомі, як не відомо хто є відповідальним за вказані зброї і ймовірний виток даних з реєстрів. Слід вказати , що на сьогодні не існує законів, які б регламентували роботу «Дії» та «Резерв+», встановлювали відповідальність осіб за неналежне функціонування цих застосунків і порушення прав громадян на збереження їх персональних даних. Нажаль, не існує також закону, який регламентував би роботу Міністерства цифрової трансформації України, в той час коли такі закони прийняті майже по кожному міністерству в Україні. Відсутність законодавчого підґрунтя негативно позначається на стані дотримання прав громадян на конфіденційність і збереження персональної інформації.

Слід зазначити, що в Європейському Союзі та Європейській економічній зоні діє Загальний регламент про захист даних (англ. *General Data Protection Regulation, GDPR*; Regulation (EU) 2016/679), який встановлює принципи і норми збору, збереження і захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Він також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання. GDPR передбачає існування в державах незалежного професійного органу, який фінансується з незалежних джерел і на який покладено функції контролю за дотриманням стандартів GDPR. Вказаний орган встановлює порушення стандартів зберігання та захисту персональних даних. Виносить приписи про їх усунення, накладає штрафи . Нажаль, на сьогоднішній день принципи і стандарти GDPR не імплементовані в українське законодавство, а застосунки «Дія» та «Резерв+» не відповідають європейським нормам і стандартам. Створення органу, який був би фінансово і процесуально незалежним у здійсненні нагляду за дотриманням законодавства про захист персональних даних повинно позитивно вплинути на стан прав людини в Україні.

Сьогодні важко спрогнозувати всі негативні наслідки витоку інформації з реєстрів про військовослужбовців та членів їх сімей. Відсутність або зміна даних у реєстрах безпосередньо впливає на права громадян і може потягнути за собою зростання позовів до суду від військовозобов'язаних, призовників, військовослужбовців. І в процесі захисту прав цих категорій громадян виникне необхідність у доказах та експертних висновках щодо причин і наслідків збою в роботі реєстрів.

Крім традиційних криміналістичних досліджень, важливе значення в розкритті та розслідуванні злочинів у сфері використання комп'ютерних технологій мають спеціалізовані експертизи, які реалізують низку пошукових діагностичних й ідентифікаційних завдань, що стосуються дослідження як електронно-обчислювальної техніки, так і криміналістичної інформації, яка на них міститься. Результативне розслідування злочинів у сфері інформаційно–комп'ютерних технологій та захист потерпілих в судових процесах залежить від своєчасного та правильного проведення необхідних експертних досліджень. На допомогу адвокатам мають прийти висококваліфіковані працівники експертних установ, фахівці у галузі використання комп'ютерних технологій.

Слід зауважити, що необхідно закласти законодавче підґрунтя експертній діяльності в цьому напрямку, в тому числі щодо відповідальності експерта за збереження інформації, що стосується персональних даних. Законодавством чітко невизначена відповідальність експерта саме за розголошення конфіденційних чи персональних даних, проте, відповідальність експерта за розголошення даних розслідування встановлена особливою частиною кримінального кодексу та розголошення є кримінальним правопорушенням. Так, розголошення експертом даних досудового слідства або дізнання без дозволу прокурора, слідчого або особи, що проводила дізнання згідно зі ст. 387 КК України карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації відповідальність передбачена статтею 182 КК України.

Законодавче забезпечення функціонування електронних реєстрів та застосунків, які є місцем накопичення і зберігання персональних даних громадян України є невід'ємним елементом кібербезпеки України.

Закон України «Про основні засади забезпечення кібербезпеки України» надає наступне визначення поняття «кібербезпека»: «кібербезпека – захищеність життєвоважливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Даним Законом України також визначається, що «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних

систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

На основі раніше наданого визначення інформаційної безпеки, як «стану захищеності життєвоважливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» можна визначити наступні об'єкти інформаційних загроз: життєвоважливі інтереси людини; життєвоважливі інтереси суспільства; життєвоважливі інтереси держави; інформація, а точніше її властивості – вплив на свідомість та підсвідомість людини, неповноту, невчасність та невірогідність; цілісність, конфіденційність та доступність інформації.

Несумнівно, дані про військовослужбовців та членів їх сімей є об'єктом інформаційної загрози, тому необхідно комплексно та всебічно аналізувати негативні наслідки застосування інформаційних технологій, можливості несанкціонованого розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації про людей.

Для забезпечення виконання Закону України «Про захист персональних даних», слід привести українське законодавство у відповідність до європейських норм права, зокрема GDPR. Керівництву державних органів слід виробити чіткий та простий алгоритм дій співробітників, направлений на забезпечення збереження інформації про громадян у випадках форс-мажорних обставин, які спричиняють загрози кібербезпеці. Такий алгоритм дій може включати як технічні блокування доступу до реєстрів, так і вчасне реагування співробітників на місцях. Крім того, важливим є якісне законодавче підґрунтя та нормативне врегулювання функціонування комплексних інформаційно-аналітичних систем в державних органах і інституціях, яке б містило запобіжні норми щодо розміщення інформації, використання віртуальних чи матеріальних сховищ інформації, володіння та розпорядження інформаційними системами та носіями. Для цього необхідна підготовка та ретельний відбір співробітників, які будуть експертами в галузі кібернетики і користування інтернет ресурсами. Крім того, створення незалежного наглядового органу у сфері нагляду за захистом персональних даних також потребує експертів з високим рівнем технічної підготовки, правом доступу до державної таємниці і відповідною відповідальністю. Підсумовуючи можна зробити висновок що сучасні напрями розвитку судова експертиза та криміналістики повинні включати в себе напрями захисту персональних даних, в тому

числі персональних даних військовослужбовців, які як було показано вище, є недостатньо захищеними в наш час.

Література:

1. «Про основні засади забезпечення кібербезпеки України»: ВР України. Закон України від 05.10.2017 № 2163-VIII // База даних Законодавство України / URL: https://zakon.rada.gov.ua/laws/show/2163-19#top

2. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: ВР України. Закон України від 09.01.2007 № 537-16 // База даних Законодавство України / URL: https://zakon.rada.gov.ua/laws/show/537-16#Text 48

3. .https://r.search.yahoo.com/_ylt=AwrkLdgca7tmowQAYpwM34lQ;_ylu=Y29sbwNpcjIEcG9zAzEEdnRpZAMEc2VjA3Ny/RV=2/RE=1724768285/RO=10/RU=https%3a%2f%2fnv.ua%2fukr%2fukraine%2fevents%2fmobilizaciya-2024-shcho-treba-znati-pro-zastosunok-rezerv-novini-ukrajini-50419998.html/RK=2/RS=oJ2Y28HPnQf74VMSfAO9wgCX0qk-

4. https://r.search.yahoo.com/_ylt=AwrLNHm_brtmrgQAuToM34lQ;_ylu=Y29sbwNpcjIEcG9zAzYEdnRpZAMEc2VjA3Ny/RV=2/RE=1724769216/RO=10/RU=https%3a%2f%2fwww.ukr.net%2fnews%2fdetails%2ftechnologies%2f105458151.html/RK=2/RS=uHwbvDCOlA3nUi2wTxtvi_pl3Lk-

5. Кримінальний к*одекс України; Кодекс, Закон* від 05.04.2001 № 2341-III.

ОБҐРУНТУВАННЯ ПОСИЛЕННЯ МАЙНОВОЇ ВІДПОВІДАЛЬНОСТІ ПОРУШНИКА ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Бутнік-Сіверський Олександр,
доктор економічних наук, професор, головний науковий співробітник відділу промислової власності та комерціалізації об'єктів інтелектуальної власності
Науково-дослідного інституту інтелектуальної власності Національної академії правових наук України, судовий експерт
https://orcid.org/0000-0003-2492-231X

Економічна експертиза у сфері інтелектуальної власності (спец. 13.9 «Економічні дослідження у сфері інтелектуальної власності») – *це дослідження на основі спеціальних знань з економіки інтелектуальної власності* та здійснюється з урахуванням відповідних вимог [1]. Спеціальні знання охоплюють питання організації підприємницької