ІНСАЙДЕРСЬКІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ У ВИКОНАВЧОМУ ПРОВАДЖЕННІ

ЛИСЕНКО Сергій Олексійович - доктор юридичних наук, професор, ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», завідувач кафедри правознавства Сєвєродонецького інституту
ORCID ID: https://orcid.org/0000-0002-7050-5536.
DOI 10.32782/LAW.2020.2.7

Статтю присвячено аналізу інсайдерських загроз інформаційній безпеці у виконавчому провадженні, зростання ролі яких обумовлено створенням в Україні інституту приватних виконавців та розвитком технологій роботи з інформацією.

Автор звертає увагу на недостатню захищеність конфіденційної інформації у виконавчому провадженні. Причиною такого стану запропоновано вважати природну обмеженість системи виявлення та попередження витоку інформації (Data Leakage Prevention, DLP-системи), яка не здатна реагувати на нові або непередбачені протоколом чинники. Окрім того, зазначена система не дозволяє дізнатися про факт її злому.

Наголошено на небезпеці надмірної впевненості приватних виконавців у тому, що їх інструменти, ключі та паролі захищають потрібні файли, оскільки динамічний характер сучасної роботи може змінити цінність файлу дуже швидко.

Проаналізовано найбільш типові інсайдерські загрози виконавчому провадженню: низький рівень дисципліни роботи з інформацією, передача інформації звільненими співробітниками, можливість адміністраторів Реєстру та державних службовців Міністерства юстиції заходити під універсальними ключами у будь-яке провадження та знаходити найбільш перспективні, з точки зору матеріальної вигоди, виконавчі провадження тощо.

Розгляд методу тотального моніторингу за діяльністю співробітників дозволив виявити його низьку ефективність та наявність ряду негативних наслідків: погіршення корпоративної культури, зниження ефективності праці.

Запропоновано файлоорієнтований підхід до реалізації інформаційної безпеки та протидії інсайдерським загрозам. Зокрема, автор пропонує механізм спостереження за даними, відстежування динаміки їх зміни та переміщення, що дозволяє створити ефект «всеохоплюючої прозорості» всієї інформації для керівника. Окрім того, зазначений підхід дає можливість оперативного реагування на загрози внаслідок отримання маркерів – сповіщень про раптову зміну в процесі обігу інформації.

Ключові слова: інформація, інформаційна загроза, інформаційна безпека, виконавче провадження, приватний виконавець, інсайдерська загроза.

Обґрунтування актуальності теми дослідження

Ось уже третій рік в Україні функціонує інститут приватних виконавців. Його втілення дозволило вирішити ряд проблем, в першу чергу – розширивши можливості громадян щодо практичного захисту своїх прав та законних інтересів. І якщо для розвинених країн світу такий механізм аж ніяк не можна назвати новелою, то як вітчизняна система правосуддя, так і пересічні громадяни України ще тільки звикають до можливостей та особливостей нового формату виконання рішень.

З огляду на особливості використовуваної приватними виконавцями інформації, зокрема належність частини цієї інформації до конфіденційної, вкрай гостро постає проблема захисту інформації в процесі виконавчого провадження. Серйозною небезпекою в зазначеному контексті, є інсайдерські загрози втрати даних. Загострюють зазначену проблему високі темпи розвитку інформаційно-комп'ютерних технологій, що в сукупності зі стрімкою модернізацією сервісів обміну інформацією породжують нові, почасти непередбачувані можливості для маніпуляції інформацією, в тому числі – з корисливою метою. Попри впровадження безпекових технологій, інформаційні загрози не втрачають своїх позицій, навпаки, з кожним роком розширюючи спектр власних можливостей. Саме тому, проблематика інсайдерських загроз втрати даних та інформаційної безпеки виконавчого провадження наразі є актуальною як в Україні, так і за кордоном.

Аналіз попередніх досліджень та публікацій за тематикою дослідження

Окремі складові проблематики протидії інсайдерським загрозам розглядали у своїх працях такі вітчизняні дослідники, як- А. С. Бевза, Г.М.Гулак, Б. А. Кормич,- І. П. Мігус, І. М. Мужик, А. Ю. Нашинець-Наумова, Т. В. Німченко, В. С. Цимбалюк, С. Ф. Філоненко. Однак, впровадження в Україні інституту приватного виконання рішень та стрімкий розвиток інформаційних технологій вимагають проведення нових досліджень, орієнтованих на пошук підходів до виявлення, локалізації та усунення інсайдерських загроз у виконавчому провадженні.

Метою дослідження є аналіз сучасних та перспективних інсайдерських загроз у виконавчому провадженні

Основний зміст дослідження

У суспільстві, де кожен громадянин оснащений високотехнологічними гаджетами, що дозволяють отримувати, зберігати та обробляти інформацію з нечуваною раніше швидкістю, інсайдерська загроза – це найбільший щоденний ризик безпеки інформації, з яким стикаються люди, змушені працювати з конфіденційною інформацією. При цьому, як не дивно, усвідомлення ролі інсайдерських загроз часто призводить до почуття хибної впевненості у розумінні проблеми та захищеності від неї. Так, наприклад, багато користувачів, які працюють у Єдиному державному реєстрі виконавчих проваджень (ЄДРВП), переконані, що встановлені програмні інструменти для припинення ексфільтрації даних, упереджують інсайдерську загрозу. Але жорстока правда полягає в тому, що кращого теперішнього часто недостатньо. Досі існує великий розрив у типовому пакеті безпеки і дійсністю. Це дедалі частіше наражає дані ЄРДВП та діяльність по примусовому виконанню рішень на небезпеку [1].

Більшість органів та осіб, які ведуть діяльність по примусовому виконанню рішень за останні кілька років, отримала свій пакет інформаційної безпеки від утримувача реєстру, тобто Міністерства юстиції. Не варто відмовлятися від цінності цих зусиль, але потрібно вказати на статистику, що демонструє постійну тенденцію до зростання інцидентних загроз. Такі зусилля наразі визначено положеннями Закону України «Про Концепцію Національної програми інформатизації» [2]. Ми регулярно дізнаємось про черговий гучний інсайдерський інцидент, який здивував, збентежив спільноту фахівців і завдав значної шкоди державному або приватному виконавцю, які були надмірно впевнені у своєму герметичному пакеті безпеки.

Майже всі звичайні засоби захисту інформації керуються політикою та правилами визначеними адміністратором Реєстру. DLP, EDR, CASB тощо мають чудову ефективність щодо пошуку, позначення та інколи навіть припинення злочинних дій на основі визначених правил та політик [3]. Так, наприклад, згадувані системи виявлення та попередження витоку інформації (Data Leakage Prevention, DLP-системи) проводять сканування можливих каналів витоку даних у реальному масштабі часу, а також можуть контролювати дії користувачів і процеси обробки та передачі інформації у межах інформаційної системи. При

цьому такі системи здатні розпізнавати інформацію за певними категоріями [4, с. 68]. Але в кращих традиціях діалектики саме в цьому і криється основна проблема, адже вони можуть шукати лише те, що їм вказано шукати. Тобто теоретично доволі стійкий та захищений механізм на практиці є доволі обмеженим. Існує ряд малопередбачуваних або взагалі непередбачуваних чинників, серед яких ключову роль відіграє антропогенний (людський) фактор. З огляду на неможливість передбачення всіх гіпотетичних способів отримання інсайдером заданого файлу або типу інформації, зловмисники та конкуренти завжди будуть на один або й кілька кроків попереду. Таким чином, захист інформації в наведеній системі характеризується низьким рівнем прогнозування загроз, що навіть за вкрай оперативного реагування дозволяє розраховувати лише на реагування постфактум, локалізацію шкоди та недопущення повторного застосування вже використаного зловмисниками каналу. Окрім того, вже сьогодні існує багато способів розшифровки даних, які традиційні рішення DLP просто не можуть охопити. Це обумовлено, у тому числі, тим, що традиційний DLP фокусується на пристроях та мережах, але такі інформаційні інструменти як Bluetooth, Airdrop тощо, не завжди відображаються на кожному пристрої або мережі.

Додатковою загрозою є надмірна впевненість значної кількості суб'єктів сфери примусового виконання рішень у тому, що їх інструменти, ключі та паролі зосереджені на потрібних файлах і потрібних даних. При цьому вони, як користувачі, створюють нові файли щодня, а динамічний характер сучасної роботи означає, що даний файл може перейти від низької вартості незавершеного провадження до високочутливої інновації, що не спрацьовує протягом одного дня. Відповідно, на практиці неможливо передбачити всі потенційно цінні, чутливі й вразливі файли та типи даних у цій діяльності. Доволі показовими є свіжі приклади, коли були затримані злочинні угруповання, які викрадали й копіювали ключі нотаріусів, реєстраторів та виконавців, з метою здійснення від їх імені незаконних реєстраційних та виконавчих дій. При цьому, неодноразовими були випадки викрадення та копіювання ключів та паролів колегами по кабінету державних виконавців або ж помічниками приватних виконавців. Після чого флешки з копійованими ключами передавались зловмисникам за винагороду, а сам власник не мав ніякої уяви про начебто вчинені ним дії [5]. Висока небезпека такого методу зловмисників полягає якраз у значній інерції процесів, що породжують суттєву відтермінованість їх виявлення. Адже можуть минути не дні, а тижні, й навіть – місяці, з моменту вчинення дії від імені постраждалих. А це, у свою чергу, не лише збільшує обсяг завданих збитків, а й ускладнює пошук каналу витоку інформації та виявлення винних.

Водночас, крім вказаних, умисно вчинених інформаційних атак, можуть бути неочевидні хибні дії, на які мало хто звертає увагу. Мова йде про копіювання інформації про хід провадження або клієнтів-стягувачів, яка традиційно не визнається особливо охоронюваною. Можливість адміністраторів Реєстру та державних службовців Міністерства юстиції заходити під універсальними ключами у будь-яке провадження, відслідковувати хід виконавчих дій та знаходити найбільш перспективні, з точки зору матеріальної вигоди, виконавчі провадження, дає широке поле для зловживань. Звичайно, такі дії не можна назвати відверто злочинними. Це більше схоже навіть не на крадіжку інформації, а на непорядну конкуренцію. Хоча такі дії суперечать Закону України «Про виконавче провадження», де чітко зазначено, що інформація виконавчого провадження має конфіденційний статус та може бути відкрита тільки сторонам провадження, стягувачу та боржнику [6]. І як наслідок, виконавець отримує дії конкурентів, які переманюють стягувачів. Іноді це навіть може набувати форми відвертого тиску з вимогою передати ті чи інші (зазвичай – особливо вигідні) провадження іншому виконавцю.

Однак, навіть якщо виконавець зміг виокремити потенційно цінні або чутливі файли зі своєї діяльності, він не може просто заблокувати їх усі, адже для цього до-

ведеться перемістити значний масив інформації. Такі речі, як вхідний пароль, ключ доступу, списки виконавчих проваджень та інформація щодо стягувачів і боржників, повинні переміщуватися між ним та його колегами, навіть поза його діяльністю, у Єдиний реєстр боржників. Таким чином, виконавець фактично створює прогалини в політиці власної інформаційної безпеки, і це, звичайно, привертає увагу зловмисників, полегшуючи їм пошук методів обходу захисту або способів отримання інсайдерських файлів.

Другий фатальний недолік звичайних засобів безпеки, таких як DLP: вони не знають, коли їх зламали. Такі засоби зосереджені на перегляді конкретних дій користувача. Якщо ж дія користувача виходить за межі визначених адміністратором правил, вони не бачать її, а отже і виконавець її не бачить. На практиці це означає, що коли зловмисники знаходять спосіб оминути DLP, виконавець, швидше за все, не матиме уявлення про загрозу і не застосує заходи боротьби. Як наслідок, у більшості випадків виконавець може виявити втрату даних лише постфактум – після настання матеріального збитку, наприклад – коли конкурент відкриває провадження на користь його стягувачів.

Вказана антропогенна загроза вимагає запровадження чітких правил користування даними у процесі виконання рішень, які слід прописувати в трудовому контракті або посадових інструкціях виконавців та їх помічників. Вся проблема з жорсткими правилами вказує на очевидне рішення – врахуйте контекст і поведінку, що стосується конкретної дії. Існує багато рішень, що зосереджуються на поведінці користувачів. Так, деякі виконавці намагаються витягнути контекст та визначити ризики, відстежуючи кожен натиск клавіші своїми працівниками. Але такий нав'язливий моніторинг працівників має свої недоліки. Зокрема, можуть виникати етичні проблеми конфіденційності, а також юридичні прецеденти, які призводять до того, що виконавцю в подальшому буде потрібна вагома причина для контролю за колегами та помічниками. Не варто забувати, що, окрім сумнівної законності, тотальний моніторинг може зашкодити корпоративній культурі, знизити задоволеність персоналу і навіть вплинути на продуктивність. Більше того, як ми вже зазначали, креативність потенційного зловмисника завжди випереджає засоби контролю, що ще більше знижує ефективність тотального моніторингу.

Зважаючи на наведене, у своїй діяльності автор застосовує дещо інший підхід. Він спостерігає за даними, відслідковуючи динаміку їх зміни та переміщення. Це дозволяє уникнути суб'єктивізму, адже колеги та помічники можуть обдурити, проте дані – не брешуть. Основна технологія резервного копіювання в режимі реального часу означає, що можливо постійно переглядати всі проведені дії та створені дані, тому виконавцю зрозуміло, як виглядають безпечні процеси. Якщо виконавцю трапилось щось незвичне, лише тоді він може пов'язати це із певним користувачем. Тобто ми розпочинаємо з поверхневого аналізу інформації, виявляємо незвичну деталь, процес, файл, а потім – досліджуємо їх. Це усуває проблеми конфіденційності та, зрештою, зосереджує увагу виконавця на тому, що він насправді намагається захистити – його даних [7]. Такий підхід дозволяє створити ефекти «всеохоплюючої прозорості» всієї інформації для керівника.

Звісно, «всеохоплююча прозорість» даних звучить приємно, але це само по собі не вирішує проблему виявлення реальних ризиків та загроз серед океану нормальної активності. Адже спочатку виконавцю доведеться конфігурувати систему для подання сповіщень про ризики, а потім хтось повинен буде керувати всіма цими сповіщеннями. І в такому разі команда може опинитись похованою в управлінні сповіщеннями.

Наприклад, відомо, що співробітники, які звільняються з роботи, становлять близько половини всіх випадків втрати даних інсайдерської інформації [8, 9]. Отже, варто окремо зосередити увагу саме на таких ситуаціях з потенційно високим ризиком. Автор наразі розробляє алгоритми та визначає параметри відповідного продукту, будуючи прості інструменти, такі як об'єктив нашого співробітника, який орі-

єнтується на визначені ризики. Зрештою, виконавець буде просто спостерігати за поведінкою своїх даних, використовуючи глибоку прозорість та всеохопність. Такий підхід сприятиме мінімізації зусиль, оскільки виконавець отримує маркери – сповіщення, яким він зможе довіряти та відповідно діяти.

Отож, виявлення потенційно небезпечних дій зловмисників, які оминули сучасні засоби безпеки, є надзвичайно важливим напрямом діяльності. Але виявлення – це лише перший крок. Виконавцям потрібно вміти точно визначити, що саме сталося, якою мірою це ризиковано, як мінімізувати загрозу і що для цього потрібно зробити. І виконавець не зможе дозволити собі провести кілька днів, перебираючи разом всю історію, поки його інформація та дані все ще знаходяться під загрозою [10]. Тому розроблена автором методика та алгоритм дозволить об'єднувати всю цю файлову активність та контекстну інформацію, щоб дати виконавцю чіткі відповіді. Вона має на меті поєднання адміністративно-правових та програмних заходів інформаційної безпеки. Окрім іншого, це передбачає обов'язкове копіювання створених файлів у «хмару» за допомогою URL-адреси вкладки або USB-накопичувача у певний час. По суті, це дає вам негайну відповідь на питання, куди подівся файл. Оскільки методика автоматично фіксує кожну версію кожного файлу, за допомогою належних авторизацій виконавець навіть зможе відкрити фактичний файл, про який йдеться, для оцінки його вмісту та визначення ризику. Таким чином виконавець швидше отримує остаточну інформацію, необхідну для вжиття заходів, що дозволяє зекономити головний у такій справі ресурс – час.

Висновки та перспективи подальших досліджень

З огляду на обмеженість сучасних механізмів захисту даних у контексті інсайдерських інформаційних загроз у виконавчому провадженні, запропоновано файло-орієнтований підхід. Найбільш ефективним у таких умовах видається спостереження за даними, відстежування динаміки їх зміни та переміщення. Зрештою, виконавець буде просто спостерігати за поведінкою своїх даних, використовуючи глибоку прозорість та всеохопність. Такий підхід сприятиме мінімізації зусиль, оскільки виконавець отримуватиме своєрідні маркери – сповіщення, яким він зможе довіряти та оперативно діяти.

Звісно, зазначена методика не є панацеєю, адже навіть найсильніша профілактика інколи зазнає невдачі. Будь-які засоби попередження здатні зупинити лише те, що їм запрограмовано припинити, на чому автор неодноразово акцентує увагу. Окрім того, виконавець, визначаючи пріоритетність серед наведених інструментів запобігання небезпек, неминуче створює нові прогалини у своїй системі безпеки. Все це обумовлює потребу комплексного підходу до вирішення проблеми протидії інсайдерським загрозам, у тому числі – із застосуванням різних галузей знань – правознавства, програмування, менеджменту, психології, соціології тощо.

Література

1. Про органи та осіб, які здійснюють примусове виконання судових рішень і рішень інших органів. Закон України № 1403-VIII від 02 червня 2016 р. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/1403-19#Text

2. Про Концепцію Національної програми інформатизації: Закон України №74/98-ВР від 04 лютого 1998 р. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text

3. Філоненко, С. Ф. Система попередження витоку персональних даних мережевими каналами [Текст] С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко // Ukrainian Scientific Jornal of Information Security. 2014. Vol. 20, № 3. P. 279-285.

4. Гулак Г.М. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах / Г.М.Гулак, В.А. Козачок, П.М. Складанний, М.О. Бондаренко, Б.В. Вовкотруб. Сучасний захист інформації №2(30), 2017, с. 65-71.

5. Офіційний сайт Департаменту кіберполіції Національної поліції України. – Режим доступу: https://www.cyberpolice.gov.ua

6. Про виконавче провадження. Закон України № 1404-VIII від 02 червня 2016 р. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/1404-19#Text

7. Лисенко С.О., Реконструкція, як метод оцінки та аналізу моделей інформаційної безпеки, стаття, Fundamental and Applied Reserches in practice of Leading Scientific Schools, 2015-6(12) // http://orcid.org/0000-0003-4037-9652.

8. Мігус І. П. Розголошення інсайдерської інформації як загроза економічній безпеці акціонерних товариств. Інвестиції: практика та досвід № 3/2012. с. 20-23.

9. Бевза А. С. Правове забезпечення інформаційної безпеки ринку цінних паперів в Україні: дис. ... канд. юрид. наук: 12.00.07. К., 2020. 242 с.

10. Лисенко С. Сучасні тенденції розвитку інформаційної безпеки, як об'єкта правовідносин. Публічне урядування, випуск 4/19, УДК: 340:659.4.327.88(477).

SUMMARY

The article is devoted to the analysis of insider threats to information security in enforcement proceedings, the growing role of which is due to the creation in Ukraine of the institute of private performers and the development of technologies for working with information.

The author draws attention to the lack of protection of confidential information in enforcement proceedings. The cause of this condition is proposed to be the natural limitation of the information leakage prevention and prevention system (Data Leakage Prevention, DLP-system), which is not able to respond to new or unforeseen factors. In addition, this system does not allow to learn about the fact of its hacking.

Emphasis is placed on the danger of overconfidence of private performers that their tools, keys and passwords protect the required files, as the dynamic nature of modern work can change the value of a file very quickly.

The most typical insider threats to enforcement proceedings are analyzed: low level of discipline of information handling, transfer of information by dismissed employees, possibility of Registry administrators and civil servants of the Ministry of Justice to enter any proceedings under universal keys and find the most promising enforcement proceedings. etc.

Consideration of the method of total monitoring of employees' activity revealed its low efficiency and the presence of a number of negative consequences: deterioration of corporate culture, reduced work efficiency.

A file-oriented approach to the implementation of information security and counteraction to insider threats is proposed. In particular, the author proposes a mechanism for monitoring data, tracking the dynamics of their change and movement, which allows you to create the effect of "comprehensive transparency" of all information for the head. In addition, this approach allows for rapid response to threats due to the receipt of markers - notifications of sudden changes in the circulation of information.

Key words: information, information threat, information security, enforcement proceedings, private executor, insider threat.