КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343
DOI https://doi.org/10.32782/chern.v3.2022.16

О. В. Ковальова
кандидат юридичних наук,
завідувач кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
Донецького державного університету внутрішніх справ
orcid.org/0000-0003-4555-0172

УПРАВЛІННЯ ОКРЕМИМИ РИЗИКАМИ, КОТРІ МОЖУТЬ ВИНИКНУТИ В ПРОЦЕСІ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ

В статті розглядаються особливості управління окремими ризиками, котрі можуть виникнути в процесі вдосконалення інформаційного забезпечення досудового розслідування. Зазначено, що уваги потребує вивчення видів помилок та інцидентів, котрі виникають у роботі засобів інформаційного забезпечення досудового розслідування; потенційні несвідомі помилки, котрі можуть бути допущені користувачем; способи взаємодії правоохоронного програмного забезпечення із іншими «цивільними» базами даних; можливість своєчасного виявлення інформаційних загроз оперативного характеру; встановлення кореляції баз даних та інших масивів із програмами, спрямованими та теоретичне забезпечення досудового розслідування. Корупційні ризики, здебільшого, мають місце саме на стадії досудового розслідування, що обумовлено спрощеним процесом внесення неправдивих відомостей або зміни правдивих, що матиме наслідком зміну кваліфікації кримінального правопорушення, підміну доказової інформації або фігурантів кримінального правопорушення. Підсумовано, що до основних способів уникнення ризиків в процесі вдосконалення інформаційного забезпечення досудового розслідування необхідно віднести: 1) створення техніко-програмного забезпечення, спрямованого на своєчасне встановлення фактичних та потенційних програмних помилок з метою їх виправлення/мінімізації; 2) розробка програмного забезпечення, котре сприятиме зниженню корупційних ризиків шляхом обмеження доступу стороні кримінального провадження, зацікавленій у порушенні процесу досудового розслідування та сприянні контрольним перевіркам внесених коректівів органами досудового розслідування у наявні дані; 3) створення програмного забезпечення, котре надасть можливість шляхом співставлення виділяти інформацію, котра піддається сумніву із її наступною перевіркою; 4) перевірка ілюстративної інформації шляхом співставлення із фактичним об'єктом або його попередніми фотозображеннями, достовірність яких не викликає сумнівів; 5) перевірка ілюстративної інформації шляхом співставлення із фактичним об'єктом або його попередніми фотозображеннями, достовірність яких не викликає сумнівів.

Ключові слова: ризики, досудове розслідування, інформаційне забезпечення, програмні та технічні засоби, корупція, системні помилки, кримінальне правопорушення.

Kovalova O. V. **MANAGEMENT OF POTENTIAL RISKS IN IMPROVING THE INFORMATION SUPPORT OF PRE-TRIAL INVESTIGATION**

The article considers the peculiarities of managing certain risks that may arise in the process of improving the information support of pre-trial investigation. It is noted that attention needs to be paid to the study of types of errors and incidents that occur in the work of information support means of pre-trial investigation; potential unconscious errors that may be made by the user; methods of interaction of law enforcement software with other "civilian" databases; the possibility of timely detection of informational threats of an operational nature; establishment of correlation of databases and other arrays with programs aimed at and theoretical provision of pre-trial investigation. Corruption risks, for the most part, take place precisely at the stage of pre-trial investigation, which is caused by a simplified process of entering false information or changing true information, which will result in a change in the qualification of a criminal offense, a change of evidentiary information or persons involved in a criminal offense. It is summarized that the main methods of avoiding risks in the process of improving the information support of the pre-trial investigation should include: 1) creation of technical and software aimed at the timely establishment of actual and potential software errors in order to correct/minimize them; 2) development of software that will contribute to the reduction of corruption risks by limiting access to the party of criminal proceedings interested in violating the pre-trial investigation process and facilitating control checks of the corrections made by the pre-trial investigation bodies to the available data; 3) creation of software that will make it possible to identify questionable information by comparing it with its subsequent verification; 4) verification of illustrative information by comparison with the actual object or its previous photographs, the authenticity of which is beyond doubt; 5) verification of illustrative information by comparison with the actual object or its previous photographs, the authenticity of which is beyond doubt.

Key words: risks, pretrial investigation, information support, software and technical means, corruption, system errors, criminal offense.

© О. В. Ковальова, 2022

Інформаційне забезпечення досудового розслідування на сьогоднішній день надає можливість максимально удосконалити процес розкриття кримінальних правопорушень, мінімізувавши при цьому час та зусилля, які мають прикладатись учасниками кримінального провадження. При цьому, нажаль, поряд із низкою переваг залишаються певні фактори, котрі можуть мати зворотній ефект та призводити до прийняття неправильних, позбавлених об'єктивності рішень по кримінальному провадженню. Це обумовлено наявністю певних ризиків, котрі можуть виникати в процесі вдосконалення інформаційного забезпечення досудового розслідування.

Системно-структурні ризики, котрі можуть виникнути в процесі вдосконалення інформаційного забезпечення досудового розслідування. Так, ризики можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки (так само, як і багатьох інших ризиків в економіці та управлінні) є їх поділ на: системні ризики – некеровані ризики, пов'язані з тим середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи; операційні ризики – як правило, керовані ризики, пов'язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами тощо. Всі негативні впливи на інформаційні активи, захист від яких (впливів) передбачає інформаційна безпека, можуть бути розділені на три основні види: порушення конфіденційності інформації; руйнування (втрата, необоротна зміна) інформації; недоступність інформаційних ресурсів – виникнення ситуацій, коли користувачі (всі або їх частина) на деякий період часу втрачають можливість доступу до необхідних даних (або інформаційних систем) [1, с. 23]. Таким чином, наведений перелік стосується випадків, коли інформаційні масиви зазнають певного пошкодження через помилки, котрі теоретично не мають мети порушення процесу досудового розслідування, але фактично можуть призвести до втрати доказової інформації, що може мати потенційну загрозу процесуальним строкам та рішенням, а також фінальному завершенню кримінального провадження.

Безпосереднім джерелом ризиків і негативних впливів є загрози, під якими розуміються потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що порушують інформаційну безпеку. Виділяється безліч типів загроз і безліч критеріїв для класифікації загроз інформаційній безпеці. Одним з основних таких критеріїв є розташування джерела порушень до інформаційних ресурсів, щодо яких здійснюється негативний вплив. Відповідно до цього критерію порушення можуть бути розділені: на обумовлені внутрішніми факторами (персоналом підприємства, роботою власних інформаційних систем); обумовлені зовнішніми факторами (зловмисниками, які не мають безпосереднього відношення до компанії – власника інформаційних активів, природними факторами тощо). Іншим важливим критерієм є наявність намірів здійснити порушення. Відповідно до нього виділяють: цілеспрямовані дії (можуть бути здійснені як власним персоналом, так і зовнішніми противниками); випадковий вплив (помилки користувачів та адміністраторів, зброї і випадкові порушення в роботі обладнання, непередбачений вплив природних факторів) [1, с. 24]. Вказане свідчить про те, що під час створення будь-якого засобу інформаційного забезпечення досудового розслідування (особливо – баз даних, котрі вміщують інформацію щодо основних характеристик доказів по кримінальним правопорушенням) необхідно прораховувати ризик апетит, що надасть можливість прогнозувати випадки, коли інформація має бути додатково перевірена.

На даний момент процес управління інцидентами інформаційної безпеки регламентується достатньою кількістю нормативних документів та рекомендацій. Найбільш відомими серед них є: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350 та інші. У міжнародному стандарті ISO/IEC TR 18044 [2, с. 11] наведено наступні визначення: подія інформаційної безпеки (information security event) – ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідома ситуація, яка може бути істотною для безпеки; інцидент інформаційної безпеки (information security incident) – одинична подія або ряд небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці. Інциденти ІБ можуть бути навмисними (несанкціонований доступ до інформаційних активів, незаконний моніторинг інформаційної системи, запуск шкідливих програм, обман в області послуг зв'язку (фрод, викрадення трафіку)) або випадковими (помилки користувачів комп'ютерної системи (КС), випадкові збої в роботі КС, ліній зв'язку, систем енергозбереження) [3]. Отже, що стосується інформаційного забезпечення, котре використовується правоохоронними органами, варто мати на увазі, що ризик потенційних загроз значно зростає, у зв'язку із чим актуальним напрямком його вдосконалення є створення програмного забезпечення котре надає можливість контролювати фактичні або потенційні помилки у роботі.

На практиці основними найбільш поширеними способами порушення інформаційної безпеки є: отримання несанкціонованого доступу (у тому числі і шляхом перевищення прав при санкціонованій роботі з інформаційними системами) до певних відомостей або масивів даних, поширення яких обмежене, з метою їх вивчення, копіювання, поширення, незаконного використання тощо; несанкціоноване використання інформаційних ресурсів (ресурсів обчислювальних і телекомунікаційних систем) з метою отримання вигоди або нанесення збитку (як тим системам, які незаконно використовуються, так і третім особам); несанкціонована зловмисна модифікація (зміна) даних; крадіжка грошових коштів в електронних платіжних системах і системах «клієнт-банк»; виведення з ладу (повне або часткове) програмних і апаратних засобів обробки, передачі та зберігання інформації; здійснення атак типу «відмова в обслуговуванні» – DoS (зокрема, щодо серверів в мережі Інтернет); поширення вірусів і інших шкідливих програм, що здійснюють різні негативні впливи [3]. Варто звернути увагу також на те, що нестабільною може бути і робота вторинних програм інформаційного забезпечення досудового розслідування. Ми маємо на увазі ті програмні та технічні засоби, котрі не є суто правоохоронними та використовуються на певних підприємствах, банках тощо та містять інформацію, котра може бути використана як доказова в процесі досудового розслідування.

Сучасна практика використання інформаційних систем характеризується великою кількістю і постійним зростанням числа порушень інформаційної безпеки. Одним з важливих чинників цього є постійно зростаюча доступність сучасних інформаційних технологій для злочинців, а також постійно зростаюча привабливість інформаційних систем як потенційних об'єктів нападу. Також важливою обставиною є постійне ускладнення і зростання різноманітності інформаційних систем, що використовуються, і, зокрема, програмних продуктів. З урахуванням того, що в середньому кожна тисяча рядків програмного коду може містити від 5 до 15 помилок, поява все більшого числа різних вразливостей, що створюють загрози для інформаційної безпеки, стає практично неминучою. Результатом цього є постійне зростання кількості різних порушень, пов'язаних з інформаційною безпекою. Таким чином, всі перераховані обставини: зростання різноманіття можливих порушень, збільшення їх кількості, збільшення складності інформаційних технологій, постійно зростаюча доступність комп'ютерів і телекомунікаційних засобів для злочинців – пояснюють зростання потреби власників інформаційних ресурсів (підприємств, організацій, державних відомств) у реалізації систематичних, всеосяжних заходів щодо забезпечення інформаційної безпеки [1, с. 25]. Таким чином, основне завдання процесу вдосконалення інформаційного забезпечення досудового розслідування є **створення техніко-програмного забезпечення, спрямованого на своєчасне встановлення фактичних та потенційних програмних помилок з метою їх виправлення/мінімізації.**

Окремі процеси, процедури, механізми та інструменти захисту інформації, використовувані власниками інформаційних ресурсів та інформаційних систем, можуть бути спрямовані: на обмеження і розмежування доступу; інформаційне приховування; введення надлишкової інформації і використання надлишкових інформаційних систем (засобів зберігання, обробки і передачі інформації); використання методів надійного зберігання, перетворення і передачі інформації;

нормативно-адміністративне спонукання і примус. На практиці сучасні технології захисту інформації побудовані на різних базових сервісах (таких, як автентифікація, забезпечення цілісності, контроль доступу та ін.), і використовують різні механізми забезпечення безпеки (такі, як шифрування, цифрові підписи, управління маршрутизацією тощо). Однак комплексність і масовість використання інформаційних технологій, їх інтеграція в повсякденну діяльність підприємств, організацій, урядових установ не дозволяють вирішувати завдання інформаційної безпеки тільки одними технічними засобами [1, с. 26]. Аналогічного вдосконалення потребують і відповідні технічні та програмні засоби, котрі можуть потенційно використовуватись як допоміжні у процесі досудового розслідування.

Із розвитком інформаційних технологій і інтенсифікацією інформаційного обміну організаційна та управлінська робота у сфері інформаційної безпеки виявляється спрямованою не тільки на власне захист певних інформаційних ресурсів, але і на більш «глобальний» об'єкт – створення і розвиток безпечної інформаційної інфраструктури (у різних значеннях цього терміну і з урахуванням різних його аспектів). На практиці така інфраструктура може включати в себе: надійну інфраструктуру передачі інформації і ринок послуг доступу до таких каналів зв'язку; ринок програмних і апаратних засобів, що забезпечують захист інформації; систему підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері інформаційної безпеки; загальні правила використання інформації, а також її передачі, спільної експлуатації інформаційних мереж (у тому числі протоколи інформаційного обміну); систему обміну інформацією та поширення знань про існуючі вразливості тих чи інших інформаційних технологій, про можливі загрози інформаційній безпеці та способи їх нейтралізації; законодавчу і право-

чинну систему, що забезпечує охорону майнових та інших інтересів всіх учасників інформаційного обміну; інші складові. Потреба в цілеспрямованому розвитку та підтримці такої інфраструктури породжує необхідність у виробленні специфічних організаційних і управлінських прийомів, як правило, не характерних для інформаційної безпеки в звичному («вузькому») її розумінні [1, с. 26]. Отже, уваги потребує вивчення видів помилок та інцидентів, котрі виникають у роботі засобів інформаційного забезпечення досудового розслідування; потенційні несвідомі помилки, котрі можуть бути допущені користувачем; способи взаємодії правоохоронного програмного забезпечення із іншими «цивільними» базами даних; можливість своєчасного виявлення інформаційних загроз оперативного характеру; встановлення кореляції баз даних та інших масивів із програмами, спрямованими та теоретичне забезпечення досудового розслідування.

Корупційні ризики, котрі можуть виникнути в процесі вдосконалення інформаційного забезпечення досудового розслідування. Наявність інцидентів інформаційної безпеки робить необхідним ефективне управління ними шляхом створення системи УІБ. Мета управління інцидентами безпеки: відновлення нормальної роботи служб в найкоротші терміни; зведення до мінімуму впливу інцидентів на роботу організації; забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування; зосередження ресурсів підтримки на найбільш важливіших напрямах; надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління [4, с. 57]. Основними об'єктами корупційних домовленостей на даній стадії кримінального провадження є: уникнення притягнення до кримінальної відповідальності конкретної особи у випадках, коли кримінальну справу було порушено за фактом вчинення злочину; ухилення від притягнення до кримінальної відповідальності за тяжкий злочин або зміна кримінально-правової кваліфікації з більш тяжкого злочину на менш тяжкий, а також порушення кримінальної справи за менш тяжкий злочин; уникнення застосування щодо підозрюваного або обвинуваченого запобіжного заходу у вигляді взяття під варту або зміна запобіжного заходу у вигляді взяття під варту на інший запобіжний захід, не пов'язаний з перебуванням у місцях попереднього ув'язнення; уникнення застосування заходів, спрямованих на забезпечення цивільного позову та можливої конфіскації майна (накладення арешту на майно, банківські рахунки) або зняття арешту з майна, банківських рахунків тощо; припинення розслідування (закриття кримінальної справи) за нереабілітуючими або реабілітуючими обставинами [3]. Корупційні ризики, здебільшого, мають місце саме на стадії досудового розслідування, що обумовлено спрощеним процесом внесення неправдивих відомостей або зміни правдивих, що матиме наслідком зміну кваліфікації кримінального правопорушення, підміну доказової інформації або фігурантів кримінального правопорушення.

На відміну від стадії перевірки інформації про злочин, на стадії досудового розслідування рішення про порушення кримінальної справи було прийнято і слідчий або прокурор, які розслідують кримінальну справу, мають у своєму розпорядженні увесь арсенал кримінально-процесуальних заходів, пов'язаних з розслідуванням кримінальної справи. Для осіб, щодо яких проводиться розслідування основною метою є припинити кримінальне переслідування тобто закрити кримінальну справу або, коли це не вдається, вжити заходів щодо отримання обвинувачення за менш тяжкий злочин, передбачений КК України, оскільки це суттєво вплине на вид та ступінь покарання. Крім цих глобальних цілей перед підозрюваними і обвинуваченими можуть стояти й інші цілі, які можна назвати проміжними: це – залишення на волі (обрання щодо підозрюваного або обвинуваченого запобіжного заходу, альтернативного взяттю під варту) або збереження власного майна. Суб'єктами корупційних практик на цій стадії кримінального провадження є слідчий, начальник слідчого підрозділу, прокурор, суддя, рідше – начальник і співробітники органу дізнання та судові експерти. Діяльність слідчого, начальника слідчого підрозділу та прокурора на цій стадії чітко обмежена і врегульована кримінально-процесуальним законом [5, с. 84]. Втручання у роботу засобів інформаційного забезпечення органами досудового розслідування облегшено відсутністю попередньої мотивації, у зв'язку із чим такі дії часто є латентними та встановлюються через значний проміжок часу, що може призвести до втрати необхідної інформації, котра не підлягає відновленню (наприклад, підміна даних щодо об'єктів, котрі було знищено внаслідок застосування руйнівних методів вивчення під час проведення експертного дослідження).

Слідчий має право на проведення слідчих дій, вичерпний перелік яких міститься у КПК та на прийняття рішень щодо кримінально-правової кваліфікації дій підозрюваного та обвинуваченого, необхідності та послідовності проведення слідчих дій, застосування засобів процесуального примусу, зупинення досудового розслідування та закриття кримінальної справи. Крім цього слідчий складає обвинувальний висновок і ознайомлює обвинуваченого з матеріалами кримінальної справи. Свою діяльність слідчий здійснює під організаційним та процесуальним керівництвом начальника слідчого підрозділу та процесуальним контролем і наглядом прокурора. Окремі про-

цесуальні рішення слідчий може приймати лише за згодою прокурора – обрання запобіжного заходу у вигляді взяття під варту, проведення обшуків, проведені огляду у помешканні особи, виїмка поштово-телеграфної кореспонденції та зняття інформації з каналів зв'язку, притягнення особи в якості обвинуваченого тощо. Роль судді на стадії досудового слідства полягає у винесенні постанов щодо проведення слідчих дій, які обмежують права людини: взяття під варту, проведення огляду житла та обшуку в ньому, накладення арешту на кореспонденцію та зняття інформації з каналів зв'язку, а також проведення оперативно-розшукових заходів, спрямованих на втручання у особисте життя громадян [5, с. 50]. Вказане свідчить про те, що слідчий має фактичний доступ до основного доказового масиву, окрему частину якого він сам вносить в електронні інформаційні системи.

До суду також може бути оскаржена постанова про порушення кримінальної справи. Бенефіціарами корупційних практик на даній стадії кримінального провадження виступають підозрюваний, обвинувачений та його представники – рідні, близькі тощо. Роль посередника при здійсненні корупційних домовленостей на цій стадії кримінального провадження може відігравати адвокат. Суб'єкти та бенефіціари корупційних практик на стадії досудового розслідування мають різну ступінь зацікавленості до участі в корупційних практиках і проявляють різну ступінь активності щодо ініціювання та здійснення корупційних практик, а також мають різні ролі при їхній реалізації. Наведені нижче дані дають певне уявлення щодо характеру та ступені участі різних суб'єктів кримінального провадження та осіб, що тим або іншим чином мають до нього відношення у корупційних практиках [5, с. 51]. Варто звернути увагу на те, що хоча адвокат і має обмежений доступ до окремих засобів інформаційного забезпечення, однак він може напряму співпрацювати зі слідчим з метою фальсифікації окремих даних, тим самим вибудовуючи складну систему корупційних взаємозв'язків. Таким чином, способом удосконалення інформаційного забезпечення може стати **розробка програмного забезпечення, котре сприятиме зниженню корупційних ризиків шляхом обмеження доступу стороні кримінального провадження, зацікавленій у порушенні процесу досудового розслідування та сприянні контрольним перевіркам внесених корективів органами досудового розслідування у наявні дані.**

Таким чином, проведене дослідження дозволило підсумувати, що до основних способів уникнення ризиків в процесі вдосконалення інформаційного забезпечення досудового розслідування необхідно віднести: 1) створення техніко-програмного забезпечення, спрямованого на своєчасне встановлення фактичних та потенційних програмних помилок з метою їх виправлення/мінімізації; 2) розробка програмного забезпечення, котре сприятиме зниженню корупційних ризиків шляхом обмеження доступу стороні кримінального провадження, зацікавленій у порушенні процесу досудового розслідування та сприянні контрольним перевіркам внесених корективів органами досудового розслідування у наявні дані; 3) створення програмного забезпечення, котре надасть можливість шляхом співставлення виділяти інформацію, котра піддається сумніву із її наступною перевіркою; 4) перевірка ілюстративної інформації шляхом співставлення із фактичним об'єктом або його попередніми фотозображеннями, достовірність яких не викликає сумнівів; 5) перевірка ілюстративної інформації шляхом співставлення із фактичним об'єктом або його попередніми фотозображеннями, достовірність яких не викликає сумнівів.

Література

1. Управління інформаційною безпекою: конспект лекцій: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Електронні текстові дані. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

2. Information technology – Security techniques – Information security incident management (IDT) : ISO/IEC TR 18044:2004. 76 с.

3. Копитін Ю. Розслідування інцидентів інформаційної безпеки. URL: https://ela.kpi.ua/bitstream/123456789/9600/1/11.pdf

4. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 2009. 143 с.

5. Корупційні ризики в кримінальному процесі та судовій системі / М.В. Буроменський, О.В. Сердюк, І.М. Осика та ін. Інститут прикладних гуманітарних досліджень, МАКонсалтинг. К. Москаленко О.М. ФОП, 2009. 220 с.