Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення системи ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ

УДК 340.5:351.86

ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В НІМЕЧЧИНІ: ЕВОЛЮЦІЯ ТА СУЧАСНИЙ СТАН

Володимир Сідак

Інститут захисту інформації з обмеженим доступом Національної академії Служби безпеки України

Анотація: **Розкриваються питання історії становлення системи захисту інформації з обмеженим доступом в Німеччині в XX ст.**

Summary: **The question of history of information protection basis in Germany in XX cent. is observed.**

Ключові слова: **Захист інформації з обмеженим доступом, технічний захист інформації, персональні дані про громадян, комерційна таємниця, криптографічний захист інформації, державні секрети.**

Вступ

На сьогодні питання захисту інформації набувають нового значення і стають дедалі актуальнішими. Зазначимо, що першочерговими стають проблеми захисту різних видів інформації з обмеженим доступом: персональних даних, комерційної, службової, державної таємниці тощо.

Розв'язати проблему захисту всіх видів інформації у наш час, на думку автора, неможливо без допомоги й координації держави. Вважаємо, що саме держава має створити й постійно вдосконалювати єдину систему органів із захисту інформації, до компетенції яких входив би як сам процес захисту інформації, так і надання допомоги в цьому приватним та юридичним особам.

Більше того, потрібні структури, які б займалися тестуванням, стандартизацією та сертифікацією засобів забезпечення безпеки всіх видів інформації з обмеженим доступом. У переважній більшості країн Західної Європи налагоджена чітка система захисту інформації. Деякі держави досягли в цьому напрямку більше, інші – менше. У багатьох із них в організації системи захисту інформації є унікальні, нікому більше не притаманні риси.

В українській історіографії зазначене питання досліджене недостатньо, з огляду на те, що система захисту інформації з обмеженим доступом у нашій державі перебуває на етапі становлення, а її дослідники в стані активного наукового пошуку. Дослідження організації системи захисту інформації провідних країн світу, зокрема в Німеччині, з метою поширення досвіду на нашу країну є актуальним як з наукового, так і з практичного погляду. Саме тому в роботі окреслено й проаналізовано еволюцію та організацію системи захисту інформації в Німеччині, зокрема, питання криптографічного, технічного, організаційно-правового захисту інформації [1].

Основна частина

Німеччина – одна з найбільш розвинутих країн Західної Європи в галузі інформаційної безпеки. Ця країна має розвинуту структуру органів, які займаються захистом різних видів інформації з обмеженим доступом. Від самого початку створення цієї системи захисту інформації увага була направлена на захист від промислового шпигунства й охорону державних секретів. Характерною особливістю для цієї країни є те, що установи, які вперше займалися окресленими питаннями, почали створюватися ще в 19 столітті. Наступним етапом у становленні німецької системи захисту інформації став початок XX століття. Адже відомо, що саме в Німеччині в 1914 – 1918 роках під час Першої світової війни, особливо в армії, була достатньо сильною й передовою на той час система криптографічного захисту інформації, що значною мірою посприяло перемозі на східному фронті. Зазначимо, що до Першої світової війни тільки Франція та

Австро-Угорщина мали свої дешифрувальні органи. Створення при Генеральному штабі Австро-угорської армії в 1911 році криптографічного бюро на чолі з капітаном Андрашем Фіглем було значним кроком уперед на шляху криптографічного захисту інформації в армії [2].

Відомо, що поразка російських армій під керівництвом генерала Ранненкампфа та генерала Самсонова біля Мазурських озер була викликана браком криптосистем у російській армії й навпаки наявністю їх в армії німецького блоку. Саме це дало змогу німцям вперше в історії отримати перемогу в битві, на результат якої переважним чином вплинули їх досягнення в галузі криптографії. Про це писав Гофман, один із розробників цієї операції в книзі «Війна втрачених можливостей»: «Російська радіостанція передала наказ у незашифрованому вигляді, і ми перехопили його. Це був перший з низки інших численних наказів, що передавалися у росіян на перших порах з неймовірною легковажністю... Така легковажність дуже полегшила нам ведення війни на сході, іноді лише завдяки цьому і взагалі можна було проводити операції» [3]. Більшість повідомлень та зашифрованих відомостей російських військових, які перехоплювали німці, дуже швидко дешифровувалися.

Таким чином, точне розшифрування російських криптограм дало змогу країнам німецького союзу час від часу вживати таких заходів, які впливали на результат військових операцій.

Із середини XX століття Німеччина багато уваги приділяла захисту такого виду інформації, як персональні дані. В 1970 році прийнято перший у світі нормативний акт, який регулював питання захисту персональних даних. Цей нормативний акт був запропонований федеральною землею Гесен, ініціативу через деякий час підтримали й інші федеральні землі [3]. Земельний уряд Гесен розробив законопроект про захист даних у галузі адміністративного управління. Цей закон передбачав два основних завдання: по-перше, попередити втручання у приватну сферу громадян Німеччини за допомогою нової інформаційної техніки, а по-друге, не допустити змін визначених конституцією країни розподілу повноважень у зв'язку з виникненням «інформаційних переваг» виконавчих органів влади перед парламентськими органами. Федеральний закон у цій сфері діє з 1977 року.

Із цього ж року громадяни Німеччини з приводу розголошення своїх персональних даних мають право самостійно приймати рішення, а захист їх прав з цього питання здійснює незалежний уповноважений із захисту персональних даних, якого обирають у Ландтазі.

Відповідно до редакції закону про захист персональних даних 1991 року, персональні дані перебувають під захистом тільки тоді, коли вони застосовуються в приватному житті й виконують певну громадську чи економічну функцію життєдіяльності. Зовнішній контроль за забезпеченням захисту персональних даних здійснює федеральний уповноважений із захисту персональних даних, якого обирає Бундестаг Німеччини. Він нікому не підпорядковується, а до його компетенції належить перевірка особистих скарг громадян про незаконне використання їхніх особистих даних федеральними державними установами й правоохоронними органами. Зазначимо, що інститут уповноваженого є незалежним від усіх державних органів. Таким чином, незалежність уповноважених – це гарантія свобод громадян і надійний захист від протиправних дій з боку держави.

На нижчому рівні, тобто на підприємствах, де працюють громадяни, також здійснюється захист їхніх персональних даних. Навіть на маленьких підприємствах, де працює п'ять працівників, також вводиться посада уповноваженого із захисту персональних даних. Крім того, в Німеччині забороняється збирання персональних даних громадян.

Отже, в Німеччині захист персональних даних не лише добре визначений законодавством, а й реально забезпечується в практичній діяльності й житті. Німецьке законодавство з питань захисту персональних даних базується на положеннях, які випливають із принципу інформаційного самовизначення. Тому кожний громадянин сам розпоряджається своїми персональними даними. Якщо в інтересах держави він повинен відкривати цю інформацію, то питання державних установ до нього повинні обмежуватися необхідним мінімумом, наприклад сплата податків. Використання персональних даних громадян у Німеччині заборонене. Персональні дані про громадян дозволяється збирати і використовувати тільки в рамках чітко окреслених законом цілей [4].

Багато уваги приділено в Німеччині й технічному захисту інформації. Зокрема, в інтересах інформаційної безпеки урядом Німеччини в 1993 році створено федеральне відомство із забезпечення безпеки у сфері інформаційної техніки. До компетенції цього відомства відноситься, крім технічного захисту інформації, ще й консультації громадян із питань технічного захисту інформації, а також сертифікація та стандартизація засобів безпеки. Крім того, це відомство займається пропагандою необхідності здійснювати захист інформації на підприємствах.

Слід зазначити, що на сьогодні кожне підприємство дбає про захист усіх видів інформації. З метою захисту інформації, яка циркулює на підприємстві, призначається уповноважений із її захисту. В його обов'язок входить фахове протистояння всім злочинам у комп'ютерній сфері, а також співробітництво із

правоохоронними органи, до компетенції яких входить забезпечення захисту цих питань. Природно, що на великих підприємствах в уповноваженого із захисту інформації є велика група співробітників, які допомагають йому виконувати покладені на нього функції захисту інформації.

У жовтні 1997 року в Німеччині був прийнятий Акт захисту інформації в телекомунікаціях (Teleservices Data Protection Act) (TDPA). TDPA є частиною нещодавно прийнятих положень Федерального законодавства Німеччини щодо регулювання умов інформації та комунікаційних послуг [6]. Відповідно до загальних принципів TDPA, які містяться в статті 2 Закону «Про мультизасоби інформації» (Multimedia Law), збирання, оброблення та використання інформації дозволяється лише у випадках, коли це дозволено законом або здійснюється за згодою користувача обслуговування. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач. Згода користувача не може бути умовою для надання послуг. Інформація за договором може бути зібрана, доопрацьована та використана в тому обсязі, який є необхідним для виконання договору. Персональні дані та дані бухгалтерського обліку не повинні передаватися третім особам. Однак деякі із зазначених вище типів даних можуть бути передані для певної мети обслуговування постачальників від користувачів, через яких здійснено доступ до послуг. Персональні дані та дані бухгалтерського обліку повинні бути знищені негайно після використання, як тільки потреба в таких даних відпаде. Кожен постачальник повинен запропонувати анонімне використання послуг та їх відкриту оплату. Він також повинен вжити заходів для того, аби гарантувати, що інформація використовується відповідно до правил. Крім того, користувач має бути поінформованим стосовно типу, можливостей, місця та мети збирання, оброблення та використання його даних, і він також повинен мати можливість перервати зв'язок у будь-який час.

Вище вже зазначено, що Німеччина на початку XX століття захопила лідерство у сфері криптографічного захисту інформації. У 80 – 90 роках XX ст. Німеччина створювала противагу американським спробам із впровадження систем депонування ключів і міжнародних обмежень на крипто. Ця країна відіграла помітну роль у створенні в 1997 році документа ЄС з криптографії та цифрового підпису [5]. У червні 1999 року міністр економіки і технології проголосив нову політику Німеччини в галузі криптографії. Ця політика полягала в тому, що федеральний уряд активно підтримує поширення криптографічних засобів захисту інформації. Крім того, він підтримує поширення серед громадян Німеччини, приватних підприємців і працівників місцевого управління знань із питань безпеки інформації. Федеральний уряд Німеччини підтримує німецьких програмістів, які створюють надійні криптографічні системи захисту інформації.

Традиційно в Німеччині склалися недержавна та державна системи захисту інформації. Недержавна система захисту інформації покладена на підприємства і стосується переважно захисту конфіденційної інформації, яка пов’язана з комерційною таємницею. Захистом держаних секретів займається держава.

У Німеччині немає централізованого порядку визнання права на виробничі секрети. У низці положень законів поряд з виробничими таємницями наводяться комерційні та ділові секрети. При цьому, фахівці вважають, що між цими видами (виробничими, діловими, комерційними секретами) є тільки термінологічна, а не юридична різниця. Саме тому на підприємствах створюються служби безпеки, які займаються організацією захисту комерційної таємниці та протистоять промисловому шпигунству.

Захисту державних секретів у Німеччині приділено особливу увагу. Ще у 1994 році був прийнятий закон про перевірку безпеки, на підставі якого Міністерство внутрішніх справ розробило загальну інструкцію, яка визначила умови й методи перевірки громадян, які мають доступ до секретних документів [7]. Цією інструкцією керуються уповноважені із захисту таємниці та співробітники, яким доручено перевірку секретоносіїв, а також співробітники федерального відомства із захисту конституції.

Цей нормативний акт визначає, що секретна інформація – це факти, вироби і відомості незалежно від форми їх подання, які в державних інтересах повинні зберігатися в таємниці і яким державним органом або за його дорученням наданий ступінь секретності, що відповідає необхідному рівню захисту. З метою збереження інформації в секреті їй надаються грифи: «цілком таємно», якщо ознайомлення з нею неуповноваженої особи може загрожувати існуванню або життєво важливим інтересам Німеччини чи однієї з її земель; «таємно», якщо ознайомлення з нею не уповноваженої особи може загрожувати безпеці держави або однієї з її земель чи завдати їхнім інтересам великої шкоди; «конфіденційно», якщо ознайомлення з нею неуповноваженої особи може завдати шкоди інтересам держави або однієї з її земель; «для службового користування, якщо ознайомлення з нею неуповноваженої особи може мати негативні наслідки для держави або однієї з її земель.

Для законодавства Німеччини характерна детальна розробленість системи понять різних видів таємниць, чіткі формулювання їх визначень у федеральному законодавстві. Так, відповідно до закону про умови і процедури перевірки благонадійності у ФРН (1994) секретною інформацією є факти, вироби та відомості незалежно від форми їх представлення, які в державних інтересах повинні зберігатися в

таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає необхідному рівню захисту: «цілком таємно», «таємно», «конфіденційно» чи «для службового користування» [7].

У систему секретної інформації Німеччини входить державна таємниця (відомості з грифом «цілком таємно» і «таємно») та відомча таємниця (відомості з грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що становлять секретну сферу приватних осіб, зумовлена інтересами зовнішньої безпеки держави.

У Кримінальному кодексі Німеччині передбачені норми, які регулюють питання покарання в разі розголошення державної таємниці (§§ 93 – 95, 97 КК) та розголошення відомчої таємниці (§ 353 b) [4].

Відповідно до Федерального відомчого закону (1953 р.) відомчою таємницею є «факти або відомості, збереження яких у таємниці обумовлене приписом закону чи постанови державного органу і які доступні лише обмеженому колу осіб».

Під «обмеженим колом осіб», на нашу думку, слід розуміти безпосередніх «секретоносіїв», тобто таких осіб, яким таємниця була довірена чи стала відома по службі. До них належать переважно службовці державних органів. У кримінальному законодавстві Німеччини встановлена диференційована відповідальність за розголошення секретної інформації залежно від форми вини.

Зазначимо, що в перевірці благонадійності відповідно до нормативно-правових актів бере участь федеральне відомство з захисту конституції, а у сфері повноважень міністерства оборони – військова контррозвідка відповідно до закону про військову контррозвідку. Федеральна розвідувальна служба, федеральне відомство з захисту конституції та військова контррозвідка здійснюють перевірку благонадійності своїх кандидатів і співробітників самостійно.

З метою належного відбору громадян та забезпечення безпеки проводиться: проста перевірка; розширена перевірка благонадійності; розширена перевірка благонадійності з аналізом відомостей.

У кінці 90-х років XX століття в Німеччині значно посилено поліцейський і контррозвідувальний режим стосовно іноземних громадян, особливо з пострадянських країн, які перебували там по лінії торгово-економічних і науково-технічних зв'язків. За ними здійснювалося спостереження як у службовий, так і позаслужбовий час. Слід зазначити, що спецслужби Німеччини активно взаємодіють із прикордонними військами, поліцейськими службами федеральних земель, митними органами, спілками підприємців, а також з іншими установами й відомствами, які відповідно до законодавства держави зобов'язані надавати відомості про іноземних громадян. Крім того, вони сприяли через Федеральний союз німецької промисловості боротьбі з промисловим шпигунством. Також спецслужби Німеччини проводять контррозвідувальні заходи у великих промислових фірмах, що підтримують ділові зв'язки з економічно розвинутими державами [6]. Персонал фірм підлягає так званій «триступеневій» системі перевірки, яка раніше застосовувалася тільки до державних службовців. Саме тому збираються відомості не лише про особу, яка перевіряється, а й про її родичів.

У грудні 1989 року в Німеччині прийнято нове положення про порядок виїзду секретоносіїв за кордон [7]. Згідно з ним усі особи, які мали доступ до секретної інформації, зобов'язані заздалегідь повідомляти співробітників, відповідальних за забезпечення режиму секретності, про свій намір відвідати іноземну державу.

Висновки

Саме таким чином у Німеччині формувалася, розвивалася й діє система захисту інформації з обмеженим доступом. І підприємства, і держава дбають про захист комерційної та державної таємниці. Чітко функціонує система заходів, спрямована на захист інформації з обмеженим доступом, зокрема її організаційно-правові, криптографічні, технічні складові.

Питання еволюції системи захисту інформації потребують подальшого розроблення, зокрема комплексного дослідження всіх нормативно-правових актів, які регулювали й регулюють порядок захисту інформації з обмеженим доступом у Німеччині в період 70 – 90 років XX ст.

Література: ***1.*** *Батурин Ю. М., Жодзишский А. М. Компьютерная безопасность. - М.: Юрид. Лит. 1991. – С. 101;* ***2.*** *Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. – М.: Новый юрист, 1998. – С. 96;* ***3.*** *Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / За заг. ред. Р. А. Калюжного. – Запоріжжя: Просвіта, 2001. – С. 52;* ***4.*** *Уголовный кодекс ФРГ / Пер. с нем. – М.: Из-во "Зерцало", 2000. – 208 с;* ***5.*** *Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. – М.: Новый Юрист, 1998;* ***6.*** *Teleservices Data Protection Act,*

http://ourworld.compuserve.com/homepages/ckune r/multimd 3. htm. 7. Доступ до інформації та електронне урядування / Автори-упорядники М. С. Демкова, М. В. Фігель. — К.: Факт, 2004. — 336 с.

УДК 681.3:34

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХОДІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Євген Скулиш, Дарія Прокоф'єва

Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

Анотація: **Подається огляд законодавчого забезпечення інформаційної безпеки при здійсненні оперативно-розшукової діяльності в Україні та інших країнах Європи.**

Summary: **This article represents the review of the ways of information security's supplying by the law during detective activity in Ukraine and other European countries.**

Ключові слова: **Законодавство, інформаційна безпека, оперативно-розшукова діяльність.**

Як складова метасистеми національної безпеки країни інформаційна безпека людини перебуває в тісному взаємозв'язку з рештою її складових – безпекою держави та суспільства. Вона забезпечується при дотриманні спільних для всієї системи принципів: законності, балансу життєво важливих інтересів особи, суспільства та держави, їх взаємної відповідальності щодо забезпечення безпеки та інтеграції з міжнародними системами безпеки, тощо. При цьому інформаційна безпека людини потрапляє до сфери оперативно-розшукової діяльності, яка різнобічно впливає на неї [1 – 2].

З одного боку, оперативно-розшукова діяльність покликана захищати життєво важливі інтереси людини в інформаційній сфері від внутрішніх та зовнішніх загроз. Це здійснюється шляхом виявлення, попередження, припинення та розкриття злочинів, що посягають на законні інформаційні інтереси особи, перш за все – на конституційні права та свободи людини і громадянина в цій сфері, а також шляхом здобуття інформації про події та дії, що створюють загрозу державній, військовій, економічній, екологічній або іншій складовій національної безпеки, оскільки це також безпосередньо пов'язано з забезпеченням інформаційної безпеки людини [3 – 4].

З іншого боку, власне оперативно-розшукова діяльність може створювати загрозу інформаційній безпеці людини у випадках:

- здійснення оперативно-розшукової діяльності без достатніх підстав або з порушеннями встановленого порядку проведення оперативно-розшукових заходів, особливо таких, що обмежують конституційні права та свободи людини і громадянина;
- використання одержаної в результаті проведення оперативно-розшукових заходів інформації для вирішення завдань, що виходять за межі компетенції органів, які здійснюють оперативно-розшукову діяльність (передусім мова йде про незаконне поширення інформації про особу);
- необґрунтованої відмови в наданні особі відомостей щодо отриманої про неї інформації або незаконне обмеження її в ознайомленні з такими відомостями;
- порушення вимог конспірації та режиму таємності інформації щодо осіб, які конфіденційно співробітничають або співробітничали з органами, що здійснюють оперативно-розшукову діяльність [4].

Вище йшлося про зловживання владою і повноваженнями як причину порушення балансу інтересів особи, суспільства та держави в інформаційній сфері. Однак в окремих випадках власне сам характер протиправних діянь, а також специфіка їх суб'єктів зумовлює конфлікт відповідних інтересів в інформаційній сфері. В свою чергу, це вимагає від правоохоронних органів застосування оперативно-розшукових заходів, які обмежують конституційні права і свободи громадян з метою забезпечення правопорядку та безпеки держави і суспільства. Передусім мова йде про зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, кореспонденцією тощо, застосування інших технічних засобів одержання інформації [4].

Відповідно до стандартів Європейського суду з прав людини для того, щоб перехоплення телефонного повідомлення або інший контроль кореспонденції не вважалися порушенням ст. 8 Європейської Конвенції про захист прав людини та основних свобод [5 – 6], воно має здійснюватися на підставі закону та як необхідне в демократичному суспільстві. Здійснення перехоплення повідомлення на підставі закону означає, що будь-яке спостереження за кореспонденцією має здійснюватися відповідно до закону, що відповідає вимогам доступності, передбачуваності та якості. За змістом принципу доступності «громадянин повинен мати можливість пересвідчитись, що прослуховування відповідає законодавчим