постійно пам'ятати. Так, знімання інформації з акустичних каналів може бути здійснено через стекла вікон, будівельні, сантехнічні, вентиляційні, теплотехнічні й газорозподільні конструкції, з використанням для передачі сигналів радіо, радіотрансляційних, телефонних і комп'ютерних комунікацій, антенних, і телевізійних розподільних мереж, охоронно-пожежної й тривожної сигналізації, мереж електроживлення й часофікації, гучномовного й диспетчерського зв'язку, ланцюгів заземлення й т. п. Випадковий пропуск хоча б одного можливого каналу витоку може звести до нуля всі витрати й зробити систему захисту неефективної неефективною.

Література: ***1.*** *Лаврентьев А. В. Организация в офисах защиты информации от утечки по техническим каналам. – Безопасность информации. – 1996. - № 3. – С. 62 – 66.* ***2.*** *Лаврентьев А. В. Анализ технических каналов утечки информации и классификация технических средств разведки.* - Безопасность информации. – *2000. - №4. – С. 32 – 38.* ***3.*** *Архипов О. Є, Луценко В. М., Худяков В. О. Захист інформації в телекомунікаційних мережах та системах зв'язку: Учеб. пособие. - К.: Політехніка, 2003 – 38 с.* ***4.*** *Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах святи.* - М.: *Энергоатомиздат, 1997. – 304 с.* ***5.*** *Куренков Е. В., Лысов А. В., Остапенко А. Н. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за сет ПЭМИ. - Защита информации.—1998. – № 4. – С. 48 – 50.* ***6.*** *Хорев А. А. Способы и средства защиты информации: Учеб. пособие.* - М.: МО РФ, *1998. – 316 с.* ***7****. Калинцев Ю. Л. Конфиденциальность и защита информации: Учеб. пособие по курсу «Радиовещание и электроакустика». – М.:МТУСИ, 1997.- 60 с.* ***8.*** *Шаповалов П. П. Поиск и оперативное пересечение негласного съема информации. – М.: ЗАО «Щит», 2000. – 83 с.* ***9****. Ярочкин В. И. Информационная безопасность. – М.: Международные отношения, 2000. – 400 с.*

УДК 65.012.8

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ПРОВІДНИХ КРАЇНАХ СВІТУ

Сергій Князєв

Інститут захисту інформації з обмеженим доступом Національної академії СБ України

Анотація: **Розглядаються деякі особливості охорони інформації з обмеженим доступом в провідних країнах світу.**

Summary: **Under research are some features of classified data protection in leading countries of the world.**

Ключові слова: **Захист інформації, інформація з обмеженим доступом.**

І Вступ

Інформація є досить специфічним продуктом. Закон України "Про інформацію" під поняттям "інформація" розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі. Встановлення й реалізація загальних норм, які регулюють відносини щодо реалізації права на інформацію різних суб`єктів і держави, порядок захисту інформації як об`єкта відносин неможливо здійснювати без чітких меж, що визначають сферу інформації як об`єкта права та потребують врахування загроз її існуванню.

Вищезазначений Закон [1] за режимом доступу поділив інформацію на відкриту та інформацію з обмеженим доступом, уповноваживши відповідні державні органи здійснювати контроль за режимом доступу до інформації. На сьогоднішній день питання захисту вітчизняних інформаційних ресурсів набувають все більшого значення. Це пов`язано з тим, що зростаюча залежність промислово розвинутих країн від джерел інформації – технічної, економічної, політичної та військової, а також рівень розвитку та ефективності використання засобів передачі та обробки цієї інформації призвів до виникнення принципово нового поняття – національні інформаційні ресурси – та до оцінки стрімкого росту їх стратегічного значення.

На початку 80-х років XX століття професор Гарвардського університету А. Еттінгер зазначав: "наступає час, коли інформація стає таким же основним ресурсом, як матеріали та енергія, отже, відносно цього ресурсу повинні бути сформульовані ті ж критичні запитання: хто ними володіє, хто в цьому зацікавлений, наскільки він доступний, можливість його ефективного використання" [2]. В реальному часі інформація об`єднала світ в єдину інформаційну систему і зараз обумовлює технічні, суспільні, політичні, соціальні та економічні системи.

Зростання інформаційних потреб держав світу вимагає використання ними ефективних систем збору

стратегічної інформації. При цьому, за словами колишнього директора ЦРУ Уїльяма Кейсі "неможливо виділити який-небудь один метод збору розвідувальної інформації та надати йому пріоритет серед інших. Найкращі результати можуть бути досягнуті лише при спільному використанні всіх існуючих можливостей отримання інформації" [3]. Врахування цього факту потребує серйозного технічного арсеналу, що застосовується для збору важливої інформації. На теперішній час, основними країнами-виробниками спецтехніки для збору конфіденційної інформації вважаються ФРН, Росія, США і Японія.

У зв`язку з цим провідні країни світу при захисті власних інформаційних ресурсів використовують відповідні комплексні системи для її охорони. Ефективність запровадження таких систем вимагає врахування досвіду провідних країн в інформаційній сфері і в вітчизняній практиці.

II Основна частина

Складовою захисту інформаційних ресурсів є забезпечення захисту інформації з обмеженим доступом, що в багатьох промислово розвинутих країнах включає здійснення комплексу заходів, спрямованих на виключення або, принаймні, утруднення витоку інформації, яка захищається.

До такого комплексу належить перш за все розробка й прийняття законодавчих актів в інформаційній сфері, що стосуються охорони державної таємниці і комерційних секретів фірм.

При цьому "комерційні секрети" як узагальнююче поняття включає й інші подібні визначення: "ділові секрети", "виробничі секрети", "торгівельні секрети", "комерційна таємниця" тощо, які використовуються в різних країнах. Зокрема, в США під поняттям "ділові секрети" розуміють – різноманітні види технічної інформації (формули, обладнання, методи, техніку і способи виробництва); в Японії – способи виробництва, продажу або іншу інформацію про технологію та бізнес тощо. Поняття "виробничі секрети" визначено в ФРН – креслення, рецептуру та інші письмові відомості, сукупність виробничого досвіду або інший факт, пов'язаний з виробництвом, в тому числі знання і досвід спеціалістів виробників, комерційні знання та досвід. До торгівельних секретів у Великобританії, США, Японії відносять інформацію, що придатна для промислового або комерційного використання, інформацію про способи виробництва, продажу тощо, а також інформацію про технології або бізнес [4].

Розробка й прийняття законодавчих актів в сфері охорони інформації з обмеженим доступом не випадково визначається як важливий захід. Історично склалося так, що першими правовими актами в інформаційній сфері були закони про охорону державної таємниці, тобто нормативні акти в галузі захисту інформації. Наприклад, у 1871 році в Німеччині для захисту вітчизняних секретів були визначені кримінально-правові заходи за злочини, пов'язані з розголошенням, передачею або втратою важливих державних документів та секретів, шпигунство та інші дії, які наносили шкоду державі. Німецьке Уложення 1871 року передбачало під загрозою каторжної тюрми (каторги) повідомлення іноземному уряду або розголошення планів укріплень, документів, актів, відомостей які необхідно було зберігати в таємниці від інших держав [5].

Крім розробки й прийняття законодавчих актів в інформаційній сфері, до заходів охорони інформації з обмеженим доступом відноситься:

видання директив і інструкцій, які регламентують режим використання інформації з обмеженим доступом на конкретних підприємствах і в установах та забезпечення реалізації їх вимог;

здійснення спеціальної перевірки осіб на допуск до роботи із документами, матеріалами й виробами, що містять інформацію з обмеженим доступом;

впровадження фізичної охорони об'єктів, на яких безпосередньо зберігаються матеріали, які необхідно захищати;

проведення профілактичних заходів тощо.

У США можливо виділити два основних суб'єкти, які визначають інформаційну політику в країні. До першого суб'єкта відноситься уряд, що вирішує всі питання, пов'язані із обмеженням доступу до інформації, що має оборонне, політичне, науково-технічне й інше важливе значення для національної безпеки. Його діяльність регламентується в директивах президента США й виданих на підставі них законів, таких як, наприклад, "Про торгівлю зброєю", "Про контроль над озброєнням", "Про шпигунство", "Про атомну енергію" й інших.

Другий суб'єкт – акціонерні й приватні фірми, компанії, які захищають інформацію, виходячи зі своїх комерційних міркувань.

З 1985 року уряд і спецслужби США розпочали впровадження комплексу довгострокових заходів контррозвідувального характеру в межах програм "Контррозвідувальна програма США", "Національна стратегічна програма безпеки" та інші [8]. Значного поширення набув метод OPSEC ("Operation Security") заснований на системному підході до забезпечення безпеки в промисловості. Цей універсальний метод застосовується для збереження як державної, так і комерційної таємниці, сприяє стійкій

конкурентноздатності американських компаній і фірм. Витік комерційних секретів американських компаній розглядається як такий самий удар "по національній безпеці, яким раніше вважались випадки, коли до рук іноземних агентів потрапляли відомості про нову систему зброї" [8].

В 1996 році в США був прийнятий закон про економічне шпигунство. Закон захищає насамперед торгові секрети і спрямований на боротьбу з промисловим шпигунством, прирівнюючи викрадення торгового секрету до федерального злочину. Крім того, ще в 1986 році у США була введена нова категорія інформації, що підлягає захисту – "потенційно конфіденційні відомості". Мова йде про несекретні й не конфіденційні дані, які за допомогою порівняння й компіляції можуть перетворитися на "конфіденційну" інформацію.

Значну увагу в США приділяють захисту науково-дослідних та дослідно-конструкторських робіт (НДДКР), що провадяться в інтересах створення як озброєнь, так і нових технологій. Витрати на інформаційну безпеку таких НДДКР становлять 20% від загальної вартості їх проведення [7]. Певні особливості є і стосовно режимних заходів щодо науково-технічної інформації в США, які відрізняються залежно від етапу проведення НДДКР. Коротко це можливо представити наступним чином.

1. На етапах фундаментальних і прикладних досліджень, що передують участі наукового центра в програмах НДДКР, більша частина робіт не закривається обмежувальними грифами. На цих етапах результати досліджень публікуються у вигляді статей у науково-технічних журналах і у вигляді відкритих монографій. Необхідність збереження високих темпів науково-технічного прогресу вимагає повноти, точності й вірогідності наукової інформації, що публікується. Ця вимога нерідко переважає над обмеженнями, що вводять "в інтересах національної безпеки".

2. Формування попередніх тактико-технічних вимог і ознайомлення з ними зацікавлених фірм і наукових центрів. Нерідко на цьому етапі обмежують грифами навіть відкриті теми, оскільки мова йде про можливість військово-технічної реалізації нової ідеї, імовірних витрат тощо. Встановлюється загальний гриф обмеження програми. Підрядник зобов'язаний оформити право на ознайомлення із такою інформацією.

3. Висновок контракту на попереднє проектування. Вимоги ті ж, що й у попередньому пункті.

4. Ухвалення рішення про початок і укладення контракту, складання тактико-технічного завдання. Проводиться деталізація елементів комплексної програми НДДКР із погляду присвоєння їм категорії обмеження доступу або визначення їх відкритими, перевірка персоналу з метою оформлення допуску до закритих робіт, встановлення "уразливих" посад і зон об'єкта.

5. Стадія безпосереднього здійснення програми й оформлення звіту. Роботи ведуться відповідно до режимних вимог. Звіт одержує вищий з обмежувальних грифів, який було надано його розділам і главам (елементам програми).

6. Наступні етапи – створення дослідних зразків, випробування, промислове виробництво – передбачають дотримання вимог режиму до того моменту, поки вище керівництво відомства не ухвалить рішення щодо публікації відомостей про дану програму НДДКР і стадій її здійснення [6].

Таким чином, на стадіях, що витікають за "незалежними" (від федеральних органів) дослідженнями, режимні вимоги посилюються, і вступає в силу критерій "захисту інтересів національної безпеки".

Категорії науково-технічної інформації, обмеження доступу до якої повинні забезпечуватися в першу чергу, визначаються до стадій проектування й виробництва, пов'язаних з розробкою детальних креслень і спеціальних методів виробництва. Ця інформація аналогічна тій, яку промислові фірми розглядають як приватну власність, і, як правило, скоріше відноситься до галузі технічних секретів виробництва, ніж до теоретичних досліджень. Головна увага приділяється забезпеченню технічної інформації, пов'язаної саме із цими етапами виробництва, і в меншій степені фундаментальним теоретичним дослідженням і пошуковим розробкам.

На практиці, в інтересах національної безпеки США нерідко застосовують обмеження в доступі до науково-технічної інформації як спробі закріпити переваги, які можуть дати ті або інші відкриття й винаходи [7].

У ФРН вдосконалення захисту інформації з обмеженим доступом здійснюється за наступними напрямами:

- вдосконалення законодавства в галузі захисту державної таємниці і секретів фірм;
- посилення органів контррозвідки й надання їм більших повноважень, у тому числі в області захисту державної таємниці;
- створення організацій "самодопомоги" у промисловості й розгортання їхньої діяльності.

Основні положення діючого в ФРН законодавства щодо боротьби з розкраданням секретів виробництва в сфері промисловості й торгівлі (промислове шпигунство) сформульовані в ряді окремих статей і параграфів у різних частинах кодексу законів. До цих законів відносяться: "Закон про боротьбу з

несумлінною конкуренцією“, “Постанова про боротьбу з підкупом не посадових осіб“, “Федеральний закон про охорону даних“ тощо.

У той же час німецькі засоби інформації часто вказують на недостатність засобів запобігання промисловому шпигунству. Однією з основних причин, які перешкоджають підвищенню ефективності боротьби із промисловим шпигунством, називається недостатність засобів покарання, передбачених законодавством ФРН.

Іншу причину недостатньої ефективності протидії промисловому шпигунству німецькі фахівці вбачають у протидії, яку промислові кола роблять спробам посилення заходів щодо охорони секретів виробництва. Справа в тому, що практичне застосування, наприклад, того ж “Закону про несумлінну конкуренцію” за свідченням ряду авторів [6] утруднено, оскільки постраждалі фірми часто уникають звертатися в судові органи з ряду причин, у тому числі побоюючись підриву своєї комерційної репутації.

Ще одним напрямом захисту інформації з обмеженим доступом в ФРН є створення об’єднаннями промисловців так званих організацій “самодопомоги“ і розгортання їх діяльності. До таких організацій відносяться “Німецький центр боротьби з фіктивними фірмами” в Гамбурзі; “Об’єднання по боротьбі з підкупами” в Бонні; “Координаційний центр щодо забезпечення безпеки в промисловості” в Кельні.

Створений в 1969 році “Координаційний центр щодо забезпечення безпеки в промисловості” є громадською організацією, субсидованою основними промисловими союзами ФРН. Завдання центра – надання допомоги окремим підприємствам і фірмам в організації служб безпеки в боротьбі з “промисловим шпигунством” іноземних держав і охороні інформації з обмеженим доступом від конкуруючих фірм.

До завдань зазначеного координаційного центру належить здійснення консультацій фірм з питань, що стосуються внутрівиробничої безпеки, зокрема:

- підтримка порядку на об’єктах (заводська охорона);
- протидія злочинності на виробництві;
- припинення саботажу й псування майна підприємства;
- боротьба зі шпигунством в області виробничих секретів.

Навіть із перерахованих завдань, які вирішує координаційний центр і його регіональні організації, відслідковується та роль, що приділяється цим організаціям у питаннях забезпечення вимог режиму в промисловості ФРН.

Крім того, в багатьох провідних країнах світу використовується практика збереження інформації з обмеженим доступом працівниками підприємств і установ за угодою, без укладання якої працівник не допускається до такої інформації, або взагалі не приймається на роботу. Зокрема, на службовців, так само як на працівників приватного сектора, нерідко покладається, за угодою, зобов`язання дотримуватися режиму при використанні інформації з обмеженим доступом.

Зобов`язання зберігати інформацію можуть поширюватись на відомості, що стосуються політики, виробничої, наукової та комерційної діяльності, винаходів, джерел постачання, а також на особисті дані співробітників. Мотиви включення в договір умови про конфіденційність відрізняються залежно від того, на кого розповсюджується вимога. Службовці можуть бути “зв`язані державною таємницею“ або зобов`язаннями, що покладені на державні органи перед громадянами – не розголошувати інформацію особистого характеру й зберігати конфіденційний характер їхніх стосунків. При цьому, умова конфіденційності в деяких випадках вступає в конфлікт із тим, що відноситься до інтересів суспільства. Суди Великобританії й Австралії визнають, що інтерес суспільства в розкритті злочинів переважує зобов`язання конфіденційності [10].

При прийомі на роботу, пов`язану з використання інформації з обмеженим доступом, в провідних країнах світу все активніше використовують можливості поліграфа, його застосовують також при проведенні розслідувань, пов`язаних з викраденням інформації з обмеженим доступом. Так, в США службовці багатьох фірм і всіх “спеціальних установ“ проходять перевірку на детекторі не рідше одного разу в півроку, причому завжди раптово. Ця обов`язкова умова обумовлюється в вищезазначеній угоді.

Сучасні поліграфи являють собою багатоцільові медико-біологічні прилади, що здатні одночасно реєструвати психофізіологічні реакції під час кількох фізіологічних процесів. Зокрема, прилад фіксує зміни при диханні, шкірно-гальванічному рефлексі, у серцево-судинній та інших системах. За весь час використання поліграфа він не зазнав принципових змін і не суттєво відрізняється від першого поліграфа, створеного Л. Кілером“ [9]. Сьогодні поряд з приладами, що здійснюють записи чорнилами, використовують комп`ютерні поліграфи американських фірм “Lafaette“, “Axciton“, з`явилися поліграфи російського виробництва фірм “Гротек“, “ЕПОС“, “Геолід-Перфур“ та корпорації “Інекс“.

Відмінними рисами комп`ютерних поліграфів є:

- наявність декількох реєстраційних каналів, які дають змогу відстежувати динаміку фізіологічних процесів під час перевірки поліграфом;
- забезпечення надійної та апробованої системи кількісної оцінки зареєстрованих показників;
- інтерфейс, що сумісний з комп`ютером;
- спеціальне програмне забезпечення для підтримання можливостей поліграфа;
- різні засоби живлення, в тому числі і автономне.

Вже з середини 90-х років XX століття поліграф застосовувався в 57 країнах світу, проте відношення до нього, з врахуванням прав людини, в провідних країнах світу неоднозначне. Зокрема, в ФРН заборонено використовувати поліграф як обов`язкову умову прийняття на роботу, що передбачає працю з інформацією з обмеженим доступом. Потребує врахування те, що поліграф не спроможний дати абсолютно вірні результати. Також, ефективність перевірок повністю залежить від майстерності оператора поліграфа, дотримання ним методичних принципів: місця, часу та тривалості проведення перевірок, видів і кількості тестів тощо.

Розвиток комп`ютерних технологій спричиняє ще одну серйозну загрозу інформації з обмеженим доступом. Бази даних та інші місця збереження "комп`ютеризованої інформації" дозволяють обробляти величезні масиви даних і забезпечують до них широкий доступ. Завдяки технологічному прогресу з таких банків даних можливо вилучати інформацію за різноманітнішою тематикою. Потенційно безмежні можливості одержання й компіляції даних викликають тривогу в провідних країнах світу за збереження в конфіденційності тих або інших відомостей. З метою охорони недоторканності особистого життя, а також під важелем комерційних і політичних інтересів в окремих країнах вже введені або запропоновані обмеження на користування базами даних. Так, до деяких баз даних у США заборонений доступ через кордон. Є обмеження на доступ до певних категорій американських баз даних з боку європейських користувачів – з метою унеможливлення несанкціонованого використання цих даних іншими країнами.

III Висновки

Проведений аналіз окремих аспектів забезпечення охорони інформації з обмеженим доступом на прикладі США та ФРН дозволяє зробити висновок про те, що в цих країнах вдалося об'єднати підсистему захисту державної та комерційної таємниці в єдину систему протидії зовнішнім загрозам. Дієздатність такої системи багато в чому реалізується за рахунок налагодженого механізму взаємодії відділів (служб) безпеки, що діють на підприємствах і в установах (у тому числі недержавного сектору) з національними спецслужбами. Виважений підхід до врахування досвіду провідних країн світу в галузі захисту інформації з обмеженим доступом повинен знайти практичне застосування в вітчизняній інформаційній сфері.

Література: ***1.*** *Закон України "Про інформацію"* ***2.*** *Громов Г. Беспилотные информационные средства // Знание сила. - № 7. – М., 1986. – с. 12 – 17.* ***3.*** *Signal. – USA, 1983. – p. 10 - 14.* ***4.*** *Клименко П. М. Інформація як об'єкт інтелектуальної власності, що потребує охорони // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України: Зб. Матеріалів наук.-практ. конф., Київ, 16 – 17 травня 2001 року. – К.: Вид-во Європ. ун-ту, 2003. – с. 283 – 289.* ***5.*** *Князєв С. О., Ботвінкін О. В., Колєснік О. А. Генезис системи охорони державної таємниці на території України: Аналітичний огляд / Вид-во НА СБ України. – К., 2005 – 88 с.* ***6.*** *Арсентьев М. В., Байков В. И. Зарубежный опыт защиты научно-технической информации при проведении научно-исследовательских работ // Проблемы информатизации. – М., 2002. - Вып. 3. - С. 31 – 42.* ***7.*** *Планы создания в США национального центра оценок контрразведывательной защиты и безопасности // Специальный выпуск по материалам иностранной печати. – М., 1991. - № 4. – с. 33 – 39.* ***8.*** *Белая книга российских спецслужб. – М.: «Обозреватель», 1996. – 272 с.* ***9.*** *Холодный Ю. И., Барченков Е. В. Использование полиграфа в интересах коммерческой безопасности // Системы безопасности. – 1996. - № 6. – с. 92 – 94.* ***10.*** *Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны. – Монография. – К.: Издательский Дом «Ин Юре», 2000. – 400 с.*