

УДК 65.012.8+34

О.В. Манжай, В.П. Коваль, Ю.М. Онищенко

Харківський національний університет внутрішніх справ, Харків

ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Досліджені концептуальні питання побудови системи захисту інформації на об'єкті інформаційної діяльності, проаналізовані окремі методи подолання системи технічної охорони, досліджені деякі аспекти побудови окремої моделі загроз.

Ключові слова: система захисту інформації, система технічного захисту інформації, система технічної охорони, окрема модель загроз, канали витоку інформації.

Вступ

Постановка проблеми. Останніми роками в Україні спостерігається підвищення уваги з боку державних органів до формалізації процесу побудови системи захисту інформації (СЗІ) на об'єктах інформаційної діяльності. І це не дивно. Адже в сучасних умовах швидкого розвитку технологій та обігу інформації без її захисту не обійтися. Під час практичного вирішення завдання побудови СЗІ нерідко доводиться стикатися з проблемою нормативної невирішеності окремих питань. Зокрема, як співвідносяться між собою система технічного захисту та система технічної охорони (СТО) об'єкту, які державні органи мають координувати, організовувати та контролювати СТО, які загрози необхідно обов'язково враховувати при складанні окремої моделі загроз в рамках побудови СТО та комплексної системи захисту інформації (КСЗІ) або комплексу технічного захисту інформації (КТЗІ) тощо?

Аналіз літератури. Основні вимоги щодо створення КСЗІ та КТЗІ викладено в [1 – 5]. Вимоги щодо встановлення режиму зберігання інформації обмеженого доступу встановлюються, наприклад, у [6] та нормативно-правових актах обмеженого доступу. Питання організації системи охорони досліджуються у джерелах [7 – 8]. Аналіз вказаних джерел дозволяє виявити певні прогалини, які виникають в ході формалізації СЗІ об'єкту інформаційної діяльності.

Метою статті є дослідження проблем, що виникають в ході побудови СЗІ та окреслення можливих шляхів їх подолання.

Основний матеріал дослідження

Як відомо комплексний захист інформації досягається проведенням відповідних *правових, організаційних та інженерно-технічних заходів*. Останні два заходи, як правило, асоціюються з технічним захистом інформації (ТЗІ), під яким розуміють діяльність, спрямовану на запобігання порушенню ці-

лісності, блокуванню та (чи) витоку інформації технічними каналами [9, п. 7.1]. Як бачимо, у самому визначенні ТЗІ закладено його мету – перешкоджання витоку інформації *саме технічними каналами*, що є окремим випадком «каналів витоку інформації», тобто потенційних напрямів несанкціонованого доступу до інформації.

В Україні основними державними органами, які безпосередньо координують, організовують та контролюють процес захисту інформації є, *по-перше*, Державна служба спеціального зв'язку та захисту інформації України (далі Держспецзв'язок) *по-друге*, Служба безпеки України.

Держспецзв'язок займається питаннями захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також криптографічного та технічного захисту інформації, СБ України – питаннями, що стосуються режиму роботи з державною таємницею та конфіденційною інформацією, яка є власністю держави.

Згідно положень Закону України «Про інформацію» від 02.10.1992 р. [10] за режимом доступу інформація поділяється на відкриту та з обмеженим доступом (рис. 1).

Виходячи з наведеного бачимо, що *режимом роботи з відкритими державними інформаційними ресурсами* ані Держспецзв'язок, ані СБ України не опікується. Саме цим можна пояснити брак нормативно-правових актів, які б встановлювали, зокрема, вимоги щодо технічної охорони об'єкту, на якому циркулює така інформація.

До речі, в одному з таких актів, а саме у п. 2.2 Додатку 2 до Наказу Міністерства фінансів України № 466 від 20.07.2004 р. «Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнання» [11] зазначено, що технологічні приміщення повинні бути обладнані системами охорони з трьома незалежними видами охоронної сигналізації: на дверях, вікнах та об'ємною сигналізацією, які

виводяться до центрального пульта в приміщенні служби охорони.

Причому дані вимоги у вищенаведеному Наказі віднесено до організаційних заходів технічного за-

хисту інформації, хоча згідно діючих стандартів та нормативно-правових актів Держспецзв'язку вони такими не є.

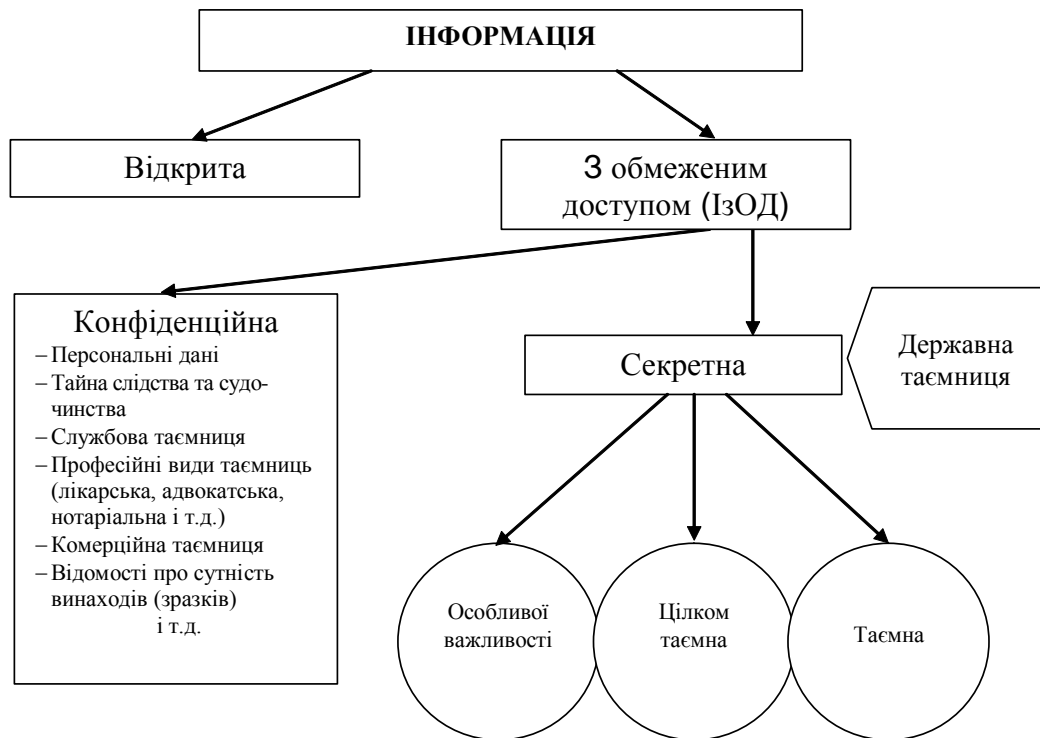


Рис. 1. Законодавча класифікація видів інформації в Україні

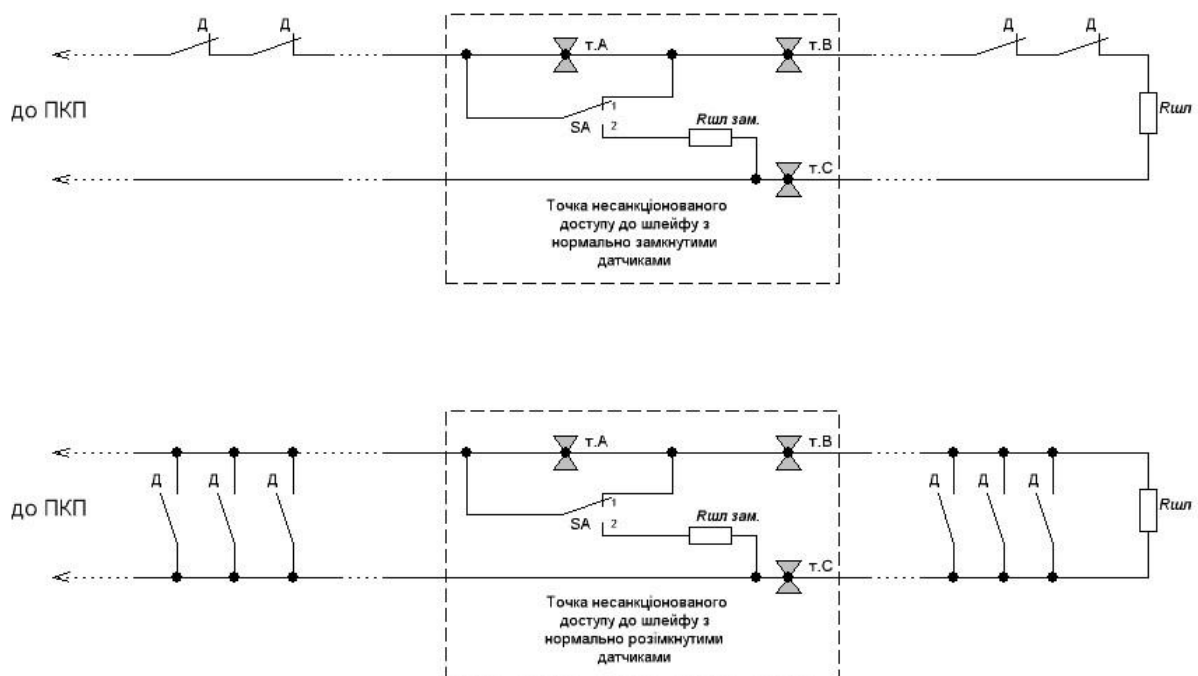


Рис. 2. Нейтралізація сигналізації з використанням кнопки перемикаючого типу

Питання регулювання СТО об'єктів інформаційної діяльності є вельми актуальним при побудові СЗІ, при цьому під час побудови СТО об'єкта необ-

хідно пройти по суті ті самі етапи, що і при побудові системи технічного захисту інформації [12, п. 3.7].

Так, при складанні окремої моделі загроз необ-

хідно враховувати багато аспектів. Зокрема треба звернути особливу увагу на можливість подолання штатних технічних засобів охорони. Найбільш вразливими елементами сучасних охоронних систем є шлейфи сигналізації (провода, кабелі) та охоронні датчики. Для демонстрації цього наведемо декілька прикладів.

Приклад 1. Припустимо, що для охорони об'єкту використовується приймально-контрольний прилад (ПКП) з часом спрацювання шлейфу 100 мс. Шлейф сигналізації розташований у загальному коробі для комунікацій або просто прокладений відкритою проводкою по стіні або стелі (що зустрічається дуже часто). Тобто зловмисник може отримати доступ до цього шлейфу.

При цьому відомі напрямки проходження шлейфу (з якого боку до шлейфу підключений ПКП і з якого – кінцевий резистор, а також номінал цього резистору).

Тоді нейтралізація такої сигналізації можлива, наприклад, з використанням звичайної кнопки перемикаючого типу (з фіксацією) та одного резистору (з номіналом, який дорівнює значенню штатного опору шлейфу ($R_{\text{шл. зам.}}$)) (рис. 2).

Основною умовою для такого способу блокування шлейфу є час перемикання контакту кнопки, який має бути менше часу реакції шлейфу ПКП, але на практиці ця вимога елементарно задовольняється. Так, наприклад, час реакції шлейфу канадського пульту РС 585 за умовчанням складає 500 мс, але може бути зменшений до 35 мс.

На першому етапі здійснюється підключення кнопки до шлейфу (рис. 2). Далі проводиться розрив шлейфу в точці А, перемикання кнопки з положення 1 в положення 2, розрив шлейфу в точці В, розрив шлейфу в точці С.

Приклад 2. Досить часто входні двері охоронюваних приміщень обладнані герконовими датчиками. Якщо ці двері вироблено з дерева, то за допомогою вірного розташування магніту навпроти такого датчику можна домогтися, щоб він не спрацював при несанкціонованому відчиненні дверей (рис. 3).

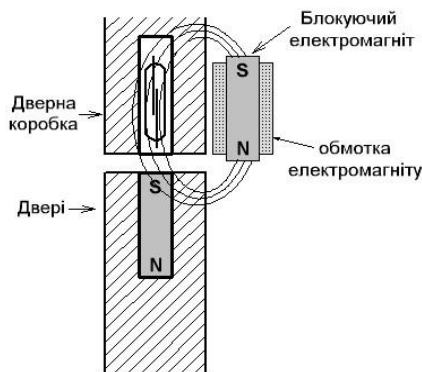


Рис. 3. Нейтралізація герконового датчика за допомогою електромагніту

Для боротьби з загрозами такого типу при створенні СТО необхідно передбачати унеможливлення доступу потенційного порушника до шлейфів та датчиків охоронної сигналізації без спрацювання самої сигналізації, наприклад, застосуванням максимальної кількості пасивних оптичних датчиків руху. Тобто забезпечити деяке резервування системи за рахунок введення надмірності.

Окреслені в прикладах загрози не є вичерпними. І, як бачимо, для ефективної побудови СТО необхідно мати якісно складену окрему модель загроз, нормативні документи щодо створення якої на даний час відсутні.

Таким чином, вироблення вірних методик створення СТО інформації є одним з ключових при побудові системи захисту інформації в цілому. Адже фізичне проникнення зловмисника на об'єкт інформаційної діяльності фактично нівелює якщо не всю, то багато рубежів системи технічного захисту інформації об'єкту. В той же час доцільним є комплексне використання охоронних систем, зокрема проводкової та безпроводової сигналізації (наприклад, на базі GSM/GPRS модему).

Окремо хотілося б зупинитися на деяких питаннях, що стосуються ТЗІ.

Так, чинні нормативно-правові акти та відомі праці фахівців в сфері технічного захисту інформації окреслюють певний перелік технічних каналів витоку інформації (ТКВІ), якими може бути порушена конфіденційність інформації з обмеженим доступом.

Таким чином, при побудові КСЗІ інформаційно-телекомунікаційних систем та комплексу ТЗІ об'єктів інформаційної діяльності, як правило, враховуються тільки визначені нормативно-правовими актами загрози, які утворюються через ТКВІ (див., наприклад [1]).

В нормативно-методичних документах та існуючих класифікаціях [13, с. 22], [14, с. 43]; [15, с. 26-37] виділяють такі найбільш загальні ТКВІ: електромагнітні та їх підвиди; хімічні та їх підвиди; акустичні та їх підвиди; вібраційні та їх підвиди; оптичні та їх підвиди.

Аналіз останніх публікацій в галузі інформаційної безпеки дозволяє говорити про актуальність відносно нового ТКВІ, який не враховується вітчизняними нормативно-методичними документами ТЗІ, – це побічні оптичні випромінювання.

Побічні канали оптичного випромінювання несуть в собі велику небезпеку через те, що зловмисник може скористатися ними, як і деякими побічними електромагнітними випромінюваннями та наведеннями, навіть не потрапляючи в межі контрольованої зони.

Додаткову складність викликає той факт, що моніторинг таких ТКВІ здійснюється за допомогою

пасивного устаткування, яке досить віддалене від цільового об'єкту спостереження.

На даний момент можна виділити по меншій мірі три відомі реалізації побічного каналу оптичного випромінювання:

1. Побічне випромінювання через світлодіодні індикатори відповідних пристроїв.
2. Побічне випромінювання з екранів моніторів з електронно-променевою трубкою (ЕПТ).
3. Змішане випромінювання.

Сутність цих реалізацій побічного каналу оптичного випромінювання така.

1. У 2002 році Джо Лорі (Joe Loughry) та Девід Умфрес (David A. Umphress) опублікували наукову статтю «Витік інформації через оптичні випромінювання» (Information Leakage from Optical Emanations), суть якої полягала в наступному. Світлодіодні індикатори, які розміщено на пристроях зв'язку, за певних умов можуть випромінювати модульований оптичний сигнал, який безпосередньо пов'язаний з передаваною інформацією. При цьому зломиснику навіть не потрібен фізичний доступ до пристрою, оскільки він може віддалено перехопити всі оброблювані пристроєм дані, включаючи початковий текст в системах шифрування інформації. Результати експериментів, наведені в статті, показали, що навіть в реальних умовах дані можуть бути перехоплені на значній відстані. Таким чином свою вразливість продемонстрували багато пристроїв, включаючи модеми та IP-маршрутизатори [16].

2. Трохи пізніше було оприлюднено статтю Маркуса Куна (Markus G. Khun) «Ризики оптичного спостереження за дисплеями ЕПТ» (Optical Time-domain Eavesdropping Risks of CRT Displays). В статті наголошувалося на реальній можливості відтворення зображення з екрану комп'ютерного монітора за відбитим зі стін світлом. Це твердження Кун обґрунтував опублікованими результатами експериментів. Інформація, яка відображається на екрані дисплеїв з електронно-променевою трубкою, може бути реконструйована за вивертаним і навіть дифузійно відбитим світлом за допомогою фотоелектронного помножувача (наприклад, Hamamatsu H6780-01) та комп'ютеру з достатньо швидким аналогово-цифровим перетворювачем [17].

3. Згадані види побічного випромінювати можуть існувати в комплексі, утворюючи, таким чином, змішане випромінювання.

Захисні заходи для блокування таких ТКВІ є доволі простими:

- заклеювання світлодіодів, наприклад, чорною електропровідною стрічкою;
- щільне зашторювання вікон при роботі з конфіденційною інформацією.

Висновки

За діючим законодавством технічний захист інформації не включає в себе технічну охорону об'єкту інформаційної діяльності, відповідно не передбачено конкретних загальнодержавних механізмів щодо ТСО відкритих державних інформаційних ресурсів, а також не встановлено відповідальних за таку охорону.

Не розроблено нормативно-методичне забезпечення щодо порядку та вимог до ТСО відкритих державних інформаційних ресурсів, зокрема не передбачено побудову відповідної окремої моделі загроз для об'єктів, де циркулює така інформація.

Для підвищення ефективності побудови КСЗІ доцільним видається:

- посилення наукових досліджень побічних каналів оптичного випромінювання;
- внесення змін до відповідних нормативно-правових актів з метою врахування побічних каналів оптичного випромінювання при побудові СЗІ;
- врахування означених ТКВІ при побудові моделі загроз для конкретного об'єкту інформаційної діяльності;
- розробка відповідних пристроїв для моніторингу таких ТКВІ відповідними суб'єктами розвідувальної діяльності України для вирішення поставлених перед ними службових задач.

Список літератури

1. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України №125 від 08.11.2005 р. – [Електронний ресурс]. – Режим доступу к док.: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=46074.
2. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. – [Електронний ресурс]. – Режим доступу к док.: <http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=71663>.
3. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. – [Електронний ресурс]. – Режим доступу к док.: <http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=71665>.
4. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. – [Електронний ресурс]. – Режим доступу к документу: <http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=71667>.

5. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. – [Електронний ресурс]. – Режим доступу к док.: <http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=71669>.

6. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави», затверджена постановою Кабінету Міністрів України № 1893 від 27.11.1998 р. [із змінами і доповненнями на 08.12.2006] // Офіційний вісник України. – 1998. – № 48 (17.12.1998). – ст. 1764.

7. Андрианов В.И. Охранные устройства для дома и офиса / В.И. Андрианов, А.В. Соколов. – СПб.: Лань, 1997. – 304 с.

8. Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации / В.Г. Синилов. – М.: Academia, 2004. – 352 с.

9. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. – [Електронний ресурс]. – Режим доступу к док.: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38934&cat_id=38836.

10. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями на 23.06.2005] // Відомості Верховної Ради України. – 1992. – № 48 (01.12.1992). – ст. 650.

11. Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнання: Наказ Міністерства

фінансів України від 20.07.2004 р. – [Електронний ресурс]. – Ліга:Еліт: Мережна версія.

12. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. – [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38883&cat_id=38836.

13. Халупин Д.Б. Защита информации. Вас подслушивают? Защищайтесь / Д.Б. Халупин. – М.: НОУ ШО БАЯРД, 2004 – 432 с.

14. Болдырев А.И. Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практическое пособие / А.И. Болдырев, И.В. Василевський, С.Е. Сталенков. – М.: ЗАО НПЦ Фирма «Нелк», 2001. – 138 с.

15. Волобуєв С.В. О систематизации выявления и анализа каналов утечки. Прямые и косвенные носители информации / С.В. Волобуєв // Вопросы защиты информации. – М.: НОУ ШО БАЯРД, 2000. – № 1. – 198 с.

16. Loughry J. Information Leakage from Optical Emanations / J. Loughry, D. Umphress. – 2002. – [Електронний ресурс]. – Режим доступу: http://applied-math.org/optical_tempest.pdf.

17. Khun M. Optical Time-domain Eavesdropping Risks of CRT Displays / M. Khun. – 2002. – [Електронний ресурс]. – Режим доступу к док.: www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf.

Надійшла до редколегії 5.03.2009

Рецензент: д-р техн. наук, проф. І.П. Захаров, Харківський національний університет радіоелектроніки, Харків.

ПРОБЛЕМНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

А.В. Манжай, В.П. Коваль, Ю.Н. Онищенко

Исследованы концептуальные вопросы построения системы защиты информации на объекте информационной деятельности, проанализированы отдельные методы преодоления системы технической охраны, исследованы некоторые аспекты построения частной модели угроз.

Ключевые слова: система защиты информации, система технической защиты информации, система технической охраны, частная модель угроз, каналы утечки информации.

PROBLEM QUESTIONS OF INFORMATION SECURITY ON THE OBJECTS OF INFORMATION ACTIVITY

O.V. Manzhai, V.P. Koval, Y.M. Onischenko

The conceptual questions of construction of the information security system are probed on the objects of information activity, the separate methods of overcoming of the technical guard system are analysed, some aspects of construction of private model of threats are probed.

Keywords: information security system, technical information security system, technical guard system, private model of threats, information leakage paths.