УДК 004.056.53

Д. Ю. Гереш

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ ТА НАВЕДЕНЬ

Вінницький національний технічний університет

Анотація

Досліджено основні методи захисту інформації від витоку каналами ПЕМВН, їх призначення та можливі недоліки. Визначено найбільш ефективне застосування засобів захисту.

Ключові слова: захист інформації, ПЕМВН, інформаційних сигнал, зашумлення, екранування.

Abstract

The main methods of information protection from leakage through TEMPEST channels, their purpose and possible shortcomings are investigated. The most effective application of means of protection is determined.

Keywords: Data protection, TEMPEST, information signal, noise masking, shielding action.

За останні декілька років велика частина підприємств перейшла від зберігання інформації в паперовому вигляді до більш зручного – цифрового формату [1]. Це призвело до виникнення нових та швидкого розвитку вже існуючих засобів, що дозволяють отримати несанкціонований доступ до інформації за допомогою технічних каналів витоку інформації. Більшість із таких засобів вимагають хоча б одноразове проникнення на територію зацікавленого підприємства, а це не завжди є простим.

Однак, одним із методів, що не вимагає безпосереднього наближення до цілі атаки є перехоплення інформації каналами побічних електромагнітних випромінювань та наведень (ПЕМВН) інформаційних сигналів в додаткових технічних засобах та сторонніх провідниках [2]. Тому виникає необхідність у здійснені відповідних заходів із забезпеченні захисту інформації від каналу витоку даним каналом.

Усі методи захисту від витоку інформації каналами ПЕМВН призначені для зменшення рівня сигналу до рівня неможливості його відновлення за межами контрольованої зони. Рівень інформаційного сигналу описується рівнянням [3]:

$$SNR = \frac{P_{\text{сигнал}}}{P_{\text{шум}}} \qquad (1)$$

Таким чином, для забезпечення допустимого рівня сигналу можна здійснювати заходи захисту щодо $P_{\text{сигнал}}$ або $P_{\text{шум}}$.

Заходи захисту, що впливають на рівень потужності сигналу називаються пасивними і призначені для зменшення рівня інформаційного сигналу. Методи дії на потужність шуму називаються активним – спрямовані на створення електромагнітних завад, що ускладнюють перехоплення інформаційного сигналу [4].

Активні методи захисту здійснюються шляхом використання електромагнітних генераторів псевдовипадкових шумів. Виділяють два типи таких генераторів. А саме:

— генератори просторового зашумлення – призначенні для створення електромагнітних коливань визначеного діапазону частот (діапазон частот можливих побічних електромагнітних випромінювань) для створення завад типу «білий шум» або псевдовипадковий шум;

— лінійного зашумлення – забезпечують маскування інформаційного сигналу, що був наведений в ДТЗС або сторонніх провідниках.

Пасивні методи захисту є більш різноманітними і поділяються на [2]:

— методи, що дозволяють зменшити інформативність сигналу;

— методи, що зменшують потужність випромінювань та наведень;

— методи екранування.

Зменшення інформативності сигналу досягається шляхом його кодування, однак даний метод не запобігає перехопленню інформації шляхом знімання інформації із випромінювань монітору [5].

Методи зменшення потужності побічних електромагнітних випромінювань є широко застосовуваними . Зменшення потужності досягається шляхом використання фільтрів та заміною електричних схем з меншим випромінюванням. Ефективним засобом зменшення потужності випромінювання є заміна дротових ліній зв'язку на волоконно-оптичні [6].

Найбільш ефективним із пасивних методів захисту, а також і дороговартісним є екранування. Екранування дозволяє не лише забезпечити ефективний захист від випромінювать, а й зменшити вплив зовнішніх електромагнітних сигналів на технічні пристрої, що знаходяться в межах контрольованої зони. Розрізняються три типу екранувань: електричного поля, магнітного поля та електромагнітного [7].

Застосування екранованих приміщень є досить ефективним засобом захисту ЕОМ, особливо при використанні подвійного чи навіть потрійного екранування, проте має і ряд недоліків. По-перше, це дуже висока вартість спорудження екранованих приміщень, особливо при необхідності забезпечення високого ступеня екранування, та значні поточні витрати на підтримання відповідного рівня захисту. По-друге, екрановане приміщення створює дискомфортні умови для працюючих в ньому. У випадку розміщення в одному екранованому приміщенні кількох ЕОМ умови праці погіршуються ще більше внаслідок відбивання та складання випромінювань від окремих ЕОМ [5].

Наявність двох методів захисту надає можливість використання різноманітного поєднання активних та пасивних методів, інколи використання пасивних методів захисту дозволяє забезпечити допустимий рівень сигналу за межами контрольованої зони. Однак, зазвичай, використовується саме поєднання обох методів, адже в сучасних умовах міських забудов контрольована зона є дуже обмеженою.

Отже, дослідивши основні методи захисту від витоку інформації каналами ПЕМВН можна зробити висновок, що найефективнішим буде застосування як активних так і пасивних методів захисту в поєднанні із ефективним розміщенням об'єкту інформаційної діяльності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов – К.: "МК-Пресс", 2005. — 288 с, ил.
2. Гавриленко О.В. «Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації» : [навчальний посібник] / О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.:ІСЗЗІ «КПІ», 2016. – 104 с.
3. ТР ТЗІ ПЕМВН – 95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом ДСТСЗІ від 09.06.1995 № 25.
4. «Особливості використання еом для обробки інформації з обмеженим доступом в сучасних умовах» . [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/16101/1/01_p84.pdf
5. Хорєв, А. А. Технічний захист інформації. Навчальний посібник для студентів ВНЗ / в 3-х томах / А.А. Хорєв. − Т. 1: Технічні канали витоку інформації. - М.: НПЦ «Аналітика», 2008. – 436 с
6. Корнейчук, В.І. Волоконно-оптичні системи передавання: підручник для вузів / В.І Корнейчук, І.П. Панфілов. – Одеса: Друк, 2001. – 436 с.
7. Панова О.В. Захист працюючих від впливу електромагнітних полів екрануванням: дис…канд. техн. наук: 05.26.01 / Панова Олена Василівна. – Київ, 2014. – 151 с.
8. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Гереш Денис Юрійович — студент групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:den.heresh@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця

Heresh D.Y. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : den.heresh@gmail.com

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia