УДК 004.8:65.05:681.5 DOI: 10.31673/2518-7678.2020.042533

Катков Ю.І., к.т.н., **Белих Є.Ю.**

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ПОБІЧНИХ КОМПРОМЕНТУЮЧИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ВІД ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Katkov Yu.I., Belykh E.Yu. New information technologies for detecting adverse compromising electromagnetic radiations from electronic computer equipment. The article deals with the problem of TEMPEST - unintentional radiation of electronic equipment, which can be intercepted by malefactors in the form of radiation of an electromagnetic parasitic wave, and which, from a security point of view, is compromising radiation because they can have compromising information. Today, the term TEMPEST is the name of a technology that includes various methods of analyzing electromagnetic compromising radiation in such a way that they can be used to recover intercepted data. The task was completed: It is known that electronic equipment creates electromagnetic fields that can interfere with radio and television reception at a considerable distance. But interference is not the only problem caused by stray electromagnetic radiation. In some cases, you can get information about the signals that are used inside the equipment, when the radiation signals are intercepted by intruders and these signals are decoded. This capability poses a problem, especially in the case of digital equipment, since remote signal recovery within the equipment can allow the reconstruction of the data that the equipment is processing. Therefore, the problem arises of determining technologies for detecting spurious electromagnetic radiation from electronic computers, which may have compromising information. The content of TEMPEST-technology is considered as a physical phenomenon of capturing and recovery of electromagnetic radiation emitted by digital equipment, and which can have compromising information. TEMPEST hardware analysis is performed, which includes various types of sensitive receivers that can monitor a wide range of frequencies, as well as a combination of hardware and software capable of processing the received signals. The analysis of various types of TEMPEST-technology is carried out, namely: Tempest-attack, Soft TEMPEST, as well as a variety of technologies for intercepting information by receiving spurious radiation of a monitor signal, searching for the necessary information on a disk, outputting information to an unused serial port; reflections of the luminous flux from the monitor screen on the walls; modeling the luminous flux in LED indicators and others. Recommendations for protection against TEMPEST technologies for companies and individuals are given.

Keywords: TEMPEST, side electromagnetic compromising radiation.

Катков Ю.І., Бєлих Є.Ю. Нові інформаційні технології виявлення побічних компроментуючих електромагнітних випромінювань від електронно-обчислювальної техніки. У статті розглядається проблема TEMPEST - ненавмисного випромінювання електронного обладнання, яке зловмисники можуть перехопити у вигляді випромінювання електромагнітної паразитного хвилі, і які з точки зору безпеки є випромінювання, які компрометують, тому, що можуть мати компрометуючу інформацію. Сьогодні поняття TEMPEST – це назва технології, що включає різні методи аналізу електромагнітного компрометуючого випромінювання таким чином, щоб їх можна було використовувати для відновлення перехоплених даних. Виконано постановка задачі: Відомо, що електронне обладнання створює електромагнітні поля, які можуть створювати перешкоди для прийому радіо і телебачення на значній відстані. Але перешкоди - не єдина проблема, яка викликана паразитних електромагнітним випромінюванням. У деяких випадках можна отримати інформацію про сигнали, які використовуються всередині обладнання, коли сигнали випромінювання перехоплюють зловмисники і ці сигнали декодуються. Ця можливість створює проблему, особливо в разі цифрового обладнання, оскільки дистанційне відновлення сигналів усередині обладнання може дозволити реконструювати дані, які обробляє обладнання. Тому виникає задача визначення технологій виявлення паразитними побічних електромагнітних випромінювань від електронно-обчислювальної техніки, які можуть мати компрометуючу інформацію. Розглядається зміст TEMPEST-технології, як фізичного явища уловлювання та відновлення електромагнітного випромінювання, що випромінюється цифровим

обладнання, і яке може мати компрометуючу інформацію. Виконується аналіз обладнання TEMPEST, яке включає в себе різні типи чутливих приймачів, які можуть контролювати широкий діапазон частот, а також комбінацію апаратного і програмного забезпечення, здатну обробляти отримані сигнали. Здійснюється аналіз різних видів TEMPEST-технології, а саме: Tempest-атака, Soft TEMPEST, а також різновиди технологій перехоплення інформації шляхом прийому паразитного випромінювання сигналу монітора, пошуку необхідної інформації на диску, виведення інформації в незадіяний послідовний порт; відображення світлового потоку від екрану монітора на стінах; моделювання світлового потоку в світлодіодних індикаторах і інші. Даються рекомендації щодо захисту від TEMPEST технологій для компаній і приватних осіб.

Ключові слова: TEMPEST, побічне електромагнітне компрометує випромінювання.

Катков Ю.И., Белых Е.Ю. Новые информационные технологии выявления побочных компрометирующих электромагнитных излучений от электронно-вычислительной техникой

В статье рассматривается проблема TEMPEST - непреднамеренного излучения электронного оборудования, которое злоумышленники могут перехватить в виде излучения электромагнитной паразитной волны, и которые с точки зрения безопасности является компрометирующим излучения потому, что могут иметь компрометирующую информацию. Сегодня понятие TEMPEST - название технологии, включающей различные методы анализа электромагнитного компрометирующего излучения таким образом, чтобы их можно было использовать для восстановления перехваченных данных. Выполнена постановка задачи: Известно, что электронное оборудование создает электромагнитные поля, которые могут создавать помехи для приема радио и телевидения на значительном расстоянии. Но помехи - не единственная проблема, вызванная паразитным электромагнитным излучением. В некоторых случаях можно получить информацию о сигналах, которые используются внутри оборудования, когда сигналы излучения перехватывают злоумышленники и эти сигналы декодируются. Эта возможность создает проблему, особенно в случае цифрового оборудования, поскольку дистанционное восстановления сигналов внутри оборудования может позволить реконструировать данные, которые обрабатывает оборудование. Поэтому возникает задача определения технологий обнаружения паразитными побочных электромагнитных излучений от электронно-вычислительной техники, которые могут иметь компрометирующую информацию. Рассматривается содержание TEMPEST-технологии, как физического явления улавливания и восстановления электромагнитного излучения, испускаемого цифровым оборудования, и которая может иметь компрометирующую информацию. Выполняется анализ оборудования TEMPEST, которое включает в себя различные типы чувствительных приемников, которые могут контролировать широкий диапазон частот, а также комбинацию аппаратного и программного обеспечения, способную обрабатывать полученные сигналы. Осуществляется анализ различных видов TEMPEST-технологии, а именно: Tempest-атака, Soft TEMPEST, а также разновидности технологий перехвата информации путем приема паразитного излучения сигнала монитора, поиска необходимой информации на диске, вывода информации в незадействованный последовательный порт; отражения светового потока от экрана монитора на стенах; моделирования светового потока в светодиодных индикаторах и другие. Даются рекомендации по защите от TEMPEST технологий для компаний и частных лиц.

Ключевые слова: TEMPEST, побочное электромагнитное компрометирующее излучение.

Вступ

Відомо, що електронні прилади такі як, наприклад, комп'ютери, смартфони, планшети, принтери випромінюють електромагнітні паразитні хвилі, що являє собою загрозу для будь-яких підприємств, тому що зловмисники можуть перехопити ці випромінюють електромагнітні паразитні хвилі, які з точки зору безпеки є компрометуючими випромінювання тому, що можуть мати компрометуючу інформацію. Звідси стає зрозумілим, що одним з можливих каналів компрометуючого випромінювання є випромінювання елементів обчислювальної техніки. Отримуючи та і декодуючи ці випромінювання можна отримати відомості про всю інформації, що обробляється в обчислювальної техніці. Такої канал витоку інформації називається каналом побічного електромагнітного випромінювання і наведення (ПЕМВН). Це назва є аналогом

європейському терміну «compromising emanation» – випромінювання, що компрометують, або терміну, що застосовується в США, Telecommunications Electronics Material Protected From Emanating Spurious Transmissions (TEMPEST) - ненавмисні випромінювання електронного обладнання.

Сьогодні поняття TEMPEST – означає назву технології, що включає різноманітні методи аналізу електромагнітного компрометуючого випромінювання таким чином, щоб їх можна було використовувати для відновлення зрозумілих даних.

Таким чином вирішення проблеми TEMPEST - ненавмисного випромінювання електронного обладнання, яке зловмисники можуть перехопити у вигляді випромінювання електромагнітної паразитного хвилі, і які з точки зору безпеки є випромінювання, які компрометують, тому, що можуть мати компрометуючу інформацію є актуальною та своєчасною задачею.

Аналіз останніх публікацій

Проблемі ненавмисного випромінювання електронного обладнання, яке зловмисники можуть перехопити у вигляді випромінювання електромагнітні паразитні хвилі, і які з точки зору безпеки є компрометуючими випромінювання тому, що можуть мати компрометуючу інформацію (TEMPEST) також іноді називають "фрікінгом Ван Екка" в честь голландського вченого Віма ван Ек(Wim van Eck), який в 1985 році вперше продемонстрував, що може легко вловлювати викиди найближчого комп'ютерного монітора і відображати їх на телевізійному моніторі. В своєї дослідницької роботі під назвою "Електромагнітне випромінювання від відеодисплеїв: ризик підслуховування?" він описав проблему існування потенційних методів перехоплення композитного сигналу відеомоніторів. Свої дослідження він продемонстрував у березні 1985 року на виставці Securecom-85 в Каннах, де показав обладнання для перехоплення випромінювань монітора. Експеримент показав, що перехоплення можливий за допомогою злегка доопрацьованого звичайного телевізійного приймача [1].

Розкриття проблеми продовжено у книзі Шпигунський улов (Spycatcher) в 1986 році Пітер Райт (Peter Wright) (колишній співробітник MI5) показав, де він показав можливості для шпигунів отримання повідомлень під час передачі кодованої інформації шляхом перехвату та декодування електромагнітні паразитні хвилі[2, 3].

В роботах Росс Андерсон і Маркус Кун (Кембріджській університет) в 1998 році, обговорювалися методи, які дозволяють програмному забезпеченню на комп'ютері управляти електромагнітним випромінюванням, яке він передає. Це програмне забезпечення можна використовувати як для атаки, так і для захисту. Щоб атакувати систему, шкідливий код може закодувати вкрадену інформацію в радіочастотному випромінюванні машини і оптимізувати її для деякої комбінації діапазону прийому, вартості приймача і скритності [4].

Метою статті є: на основі визначення технологій щодо виявлення паразитними побічних електромагнітних випромінювань від електронно-обчислювальної техніки, які що можуть мати компрометуючу інформацію розробити практичні рекомендації захисту від випромінювань, що компрометують.

Постановка завдання. Добре відомо, що електронне обладнання створює електромагнітні поля, які можуть створювати перешкоди для прийому радіо і телебачення на значної відстані. Але перешкоди - не єдина проблема, яка викликана паразитними електромагнітним випромінюванням. У деяких випадках можливе отримати інформацію про сигнали, які використовуються всередині обладнання, коли сигнали випромінювання перехоплюють зловмисники і прийняті сигнали декодуються. Ця можливість є проблемою, особливо в разі цифрового обладнання, оскільки дистанційне відновлення сигналів усередині

обладнання може дозволити реконструювати дані, які обробляє обладнання. Тому виникає завдання визначення технологій щодо виявлення паразитних побічних електромагнітних випромінювань від електронно-обчислювальної техніки, які що можуть мати компрометуючу інформацію.

Виклад основного матеріалу дослідження

Зміст TEMPEST-технології. Цікаво розглянути зміст терміну TEMPEST. Історія виникнення TEMPEST, точніше ненавмисного випромінювання електронного обладнання, своїм корінням сягає в далекий 1918 рік, коли Герберт Ярдлі (Herbert Yardley) зі своєю командою був притягнутий Збройними Силами США для дослідження методів виявлення, перехоплення і аналізу сигналів військових телефонів і радіостанцій. Дослідження показали, що обладнання має різні демаскуючі випромінювання, які можуть бути використані для перехоплення секретної інформації. З цього часу засоби радіо- і радіотехнічної розвідки стали неодмінним реквізитом шпигунів різного рівня [5].

На початку 70-х років з'явилася абревіатура TEMPEST, як назва секретної програми Міністерства Оборони США по розробці методів запобігання витоку інформації через різного роду демаскуючі і побічні випромінювання електронного обладнання. У міру розвитку технології розвивалися як засобу TEMPEST-нападу (розвідки), так і засоби TEMPEST-захисту. В даний час термін TEMPEST не є абревіатурою, а застосовується і як синонім випромінювання, що компрометують (ПЕМВН) або як назва технології, що мінімізує ризик витоку секретної інформації шляхом перехоплення і аналізу різними технічними засобами побічних електромагнітних випромінювань. У зміст поняття TEMPEST входять також стандарти на обладнання, на засоби вимірювання і контролю. В останній час цілком припустимі назви типу: TEMPEST tests, TEMPEST computer иа ін. Досить часто термін TEMPEST використовується і в контексті опису засобів нападу, що це неправильно, наприклад, TEMPEST - атака, TEMPEST - пристрій для підслуховування. Мова йде про те, що термін TEMPEST призначений для припинення побічних випромінювань, а не для їх використання. Однак, таке застосування терміну зустрічається досить часто і не призводить до неправильного тлумачення. Треба підкреслити, що розширення поняття TEMPEST збільшило і кількість його неофіційних назв, наприклад, Transient Emanations Protected from Emanating Spurious Transmissions (перехідні випромінювання, захищені від випромінюючих фальшивих передач), Transient Electromagnetic Pulse Emanation Standard (Стандарт перехідного електромагнітного імпульсного випромінювання), Telecommunications Emission Security Standards (Стандарти безпеки випромінювання телекомунікацій) [6].

Для вирішення проблеми ненавмисного випромінювання електронного обладнання в розвинених країнах були розроблені керівні документи, наприклад, в США національна TEMPEST політика була затверджена Директиві 4 Національного комітету з питань безпеки в 1981 році (National Policy on Control of Compromising Emanations), в якої встановлені стандарти TEMPEST США. У секретному документі NACSIM-5100A (National Communication Security Instruction) викладені вимоги до вимірювальних приладів та описані стандарти, методики, інструкції щодо захисту від побічних паразитних випромінювань. У США введена наступна класифікація пристроїв і систем з захистом інформації від побічних паразитних випромінювань [7]:

- Тип 1 надзвичайно безпечний і доступний тільки уряду США і затвердженим підрядникам, які повинні пройти сувору перевірку. TEMPEST Level 1 (аналог стандарту NATO AMSG-720B) - обладнання даного класу відносяться до категорії вищого ступеня секретності. Устаткування має бути затверджене Агентством Національної Безпеки США і призначений для використання тільки урядовими установами США.

- Тип 2 кілька менш безпечний, але для використання як і раніше потрібен дозвіл уряду. TEMPEST Level 2 (аналог стандарту NATO AMSG-788A) - обладнання даного класу призначене для захисту менш секретної, але критичної інформації, однак також потрібне схвалення АНБ США).
- Тип 3 призначений для загального комерційного використання. TEMPEST Level 3 - обладнання даного класу призначене для захисту нетаємної, але критичною або комерційної інформації. Устаткування реєструється NIST (National Institute of Standards and Technology).

Сертифікація TEMPEST для використання в приватному секторі є надзвичайно дорогої, і в результаті вона привела до появи нового стандарту під назвою ZONE, який більш рентабельний, але кілька менш безпечний. Сертифікація TEMPEST обладнання описана в документі Національного Агентства Безпеки NSA TEMPEST Endorsement Program.

Для отримання додаткової інформації про сертифікацію TEMPEST є Програма підтримки TEMPEST Агентства національної безпеки США.

В НАТО є аналогічний стандарт, званий стандартом лабораторних випробувань компрометуючих випромінювань AMSG 720B. У Німеччині програма TEMPEST знаходиться у веденні Національної ради з телекомунікацій. У Великобританії у штаб-квартири зі зв'язків з громадськістю (GCHQ), еквівалентної АНБ, є своя власна програма.

Сучасні досягнення в області технології виробництва радіоприймальних пристроїв дозволили створювати дуже мініатюрні чутливі приймачі. Успішно впроваджується багатоканальний прийом сигналів (як з різних напрямків, так і на різних частотах), з подальшою їх кореляційної обробкою. Це дозволило значно збільшити дальність перехоплення інформації.

Особливо бурхливий розвиток TEMPEST-технології отримали в кінці 80-х, початку 90 -х років. Це пов'язано як з усвідомленням широким загалом небезпеки TEMPEST загроз, так і з широким розвитком криптографії. Застосування при передачі інформації стійких алгоритмів шифрування часто не залишає шансів дешифрувати перехоплене повідомлення. У цих умовах TEMPEST-атака може бути єдиним способом отримання хоча б частини інформації до того, як вона буде зашифрована.

Технології TEMPEST засновані на фізичному явищі уловлювання та відновлення електромагнітного випромінювання, що випускається цифровим обладнання, і яка може мати компрометуючу інформацію. У деяких випадках можливе отримати інформацію про сигнали, які використовуються всередині обладнання, коли сигнали випромінювання перехоплюють зловмисники і прийняті сигнали декодуються. Розглянемо практичні приклад.

Комп'ютерні монітори відображають інформацію за допомогою електронної гармати для управління пікселями на екрані. Електронна гармата випускає імпульси електронів, які рухаються по екрану, вражаючи пікселі зліва направо, а також вгору і вниз багато разів в секунду. Рівень напруги, що виштовхує електрони, підвищується і знижується в залежності від того, чи повинен піксель бути світлим або темним. Цей процес генерує електромагнітні імпульси, які, в свою чергу, випромінюють електромагнітні радіохвилі або електромагнітне випромінювання, яке поширюється назовні на велике відстані.

Жорсткі диски- це ще одне джерело, тому що дані зберігаються в двійковому коді і обробляються як одиниці і нулі. Відомо, що спектр сигналів одиниць і нулів може бути розглянутий як радіохвилі, які настільки ж помітні, як відбитки пальців, навіть в комп'ютерах тієї ж марки і моделі, через незначних відмінностей у виробництві компонентів.

Комп'ютерні кабелі, телефонні лінії і погано заземлення електричні системи може діяти як приймач і передавач для електромагнітних випромінювань, що дозволяє хвилях поширюватися ще далі. Ці радіохвилі потім можуть бути захоплені активної спрямованої

антеною, подані на монітор, встановлені на нуль і розшифровані за допомогою генератора горизонтальної та вертикальної синхронізації.

Таким чином, все мікрочіпи і пристрої, такі як монітор, принтери, плати комп‘ютерів мають можливість випромінювання в будь-яку провідне середовище, наприклад, лінії електропередач, зв'язку або навіть водопровідні труби. Випромінювання містить інформацію, яку пристрій відображає, створює, зберігає або передає. Тому з правильним обладнанням та методами можна відновити всі або значну частину цих даних.

Устаткування TEMPEST. Устаткування для моніторингу TEMPEST включає в себе різні типи чутливих приймачів, які можуть контролювати широкий діапазон частот, а також комбінацію апаратного і програмного забезпечення, здатну обробляти отримані сигнали в вихідні дані. Зібрані дані часто спотворюються такими факторами, як зовнішні електромагнітні перешкоди, сигнал слабкість на відстані і часткову передачу. Розширені алгоритми можуть допомогти надати більш повну картину вихідних даних.

Перехоплення даних за допомогою віддаленої передачі - це потужний інструмент моніторингу віддаленого управління, який дозволяє таємно відстежувати всі дії на одному пристрої. або декількох цільових комп'ютерів одночасно з віддаленого центру управління. Фізичний доступ не потрібно. Додаток також дозволяє агентам віддалено захоплювати і захищати цифрові докази до фізичного входу в підозрілі приміщення.

Продаж пристроїв моніторингу за TEMPEST технологіями широкому загалу заборонена, як правило, цілком можливо, але приватні організації або особи можуть придбати технологію або навіть створити її самостійно так як конструкції і устаткування щодо легко придбати.

Аналіз видів TEMPEST-технології.

Технологія Tempest-атака. Перехоплення зашифрованих повідомлень від обладнання до його шифрування для аналізу випромінювань (приймати сигнал і демодулировать його). Застосовується фізичне явище, що будь-яка шифрувальна машина, як і будь-яка інша електрична машина, має побічні електромагнітні випромінювання, яке модулюється інформаційним сигналом ще до моменту його кодування. Для боротьби з TEMPEST-атаками розробляються спеціальні конструкції комп'ютерів, що володіють малим рівнем побічних випромінювань. Правильна конструкція зводить до мінімуму ненавмисні сигнали, що випускаються пристроєм, але деякі ненавмисні сигнали завжди будуть присутнім. У конструкції таких комп'ютерів застосовуються екранують покриття зі спеціальних матеріалів і високоефективні фільтри, розроблені з метою отримання великого загасання в широкій смузі частот. Таким чином, шляхом перехоплення і аналізу побічних випромінювань шифрувальної машини, навіть не маючи ключа для розшифровки кодованих повідомлень, отримувало всю необхідну інформацію [8, 9].

Технологія Soft TEMPEST - технологія прихованої передачі даних по каналу побічних електромагнітних випромінювань за допомогою програмних засобів. Ця технологія є розвитком TEMPEST-атак і є різновидом комп'ютерної стеганографії, тобто методу прихованої передачі корисного повідомлення в нешкідливих відео, аудіо, графічних і текстових файлах. Методи комп'ютерної стеганографії в даний час добре розроблені і широко застосовуються на практиці. Якщо технологія TEMPEST-атак базується на пасивному очікуванні, то технологія Soft TEMPEST базується на програмних закладках, які дозволяють цілеспрямовано керувати випромінюванням комп'ютера. В даний час технологія Soft Tempest включає в себе не тільки способи розвідки, але і програмні способи протидії розвідці, зокрема використання спеціальних Tempest - шрифтів, що мінімізують високочастотні випромінювання. Особливістю технології Soft Tempest є використання для передачі даних каналу ПЕМВН, що значно ускладнює виявлення самого факту

несанкціонованої передачі в порівнянні з традиційною комп'ютерної стеганографії. Дійсно, якщо для запобігання несанкціонованої передачі даних по локальній мережі або мережі Інтернет існують апаратні і програмні засоби (FireWall, Proxy server і т.п.), то засобів для виявлення прихованої передачі даних по ПЕМВН немає, а виявити таке випромінювання в загальному широкополосном спектрі (більше 1000 МГц) паразитних випромінювань ПК без знання параметрів корисного сигналу вельми проблематично. Основна небезпека технології Soft Tempest полягає в скритності роботи програми-вірусу. Така програма, на відміну від більшості вірусів не псує дані, чи не порушує роботу ПК, не виробляє несанкціоновану розсилку по мережі, а значить, довгий час не виявляється користувачем та адміністратором мережі. Тому, якщо віруси, що використовують Інтернет для передачі даних, проявляють себе практично миттєво, і на них швидко знаходиться антивірусні програми, то віруси, що використовують ПЕМВН для передачі даних, можуть працювати роками, не виявляючи себе. Технологія Soft TEMPEST має такі різновиди перехоплення інформації шляхом: прийому паразитного випромінювання сигналу монітора; пошуку необхідної інформації на диску; виведення інформації в незадіяний послідовний порт; приймання випромінювання під час роботи елементів комп'ютера; приймання модульованого струму в комп‘ютері мовою інформацією; приймання випромінювань від шин або кабелів внутрішнього з‘єднання комп‘ютера; приймання випромінювань з кабелів структурованої кабельної мережі внутрішнього з‘єднання в приміщенні; приймання оптико електронного відбивання світлового потоку від екрану монітора від стін; оптико електронного модулювання світлового потоку в світлодіодних індикаторах; геолокації комп‘ютера [8, 9].

Рекомендації щодо захисту від TEMPEST технологій. Захист пристроїв від електромагнітних випромінювань досягається декількома способами.

1) *Мінімізація витоку електромагнітних випромінювань*. У найскладніших пристроях використовуються мікрокомпоненти, які були розроблені з нуля, щоб мінімізувати виток електромагнітних випромінювань, що є основою для застосування TEMPEST технологій.

2) *Екранування приміщень*. Як правило, екранування передбачає розміщення пристроїв в клітку Фарадея, яка не допускає випадкового випромінювання.

3) *Екранування кабелів та окремих схем з конструкції обчислювальної техніки*. Це робиться шляхом створення екранів або опліток кабелів та спеціальних конструкцій джерел живлення.

4) *Заземлення корпусів обчислювальної техніки.* Зазвичай це пов'язано з металевим корпусом обчислювальної техніки, яка має заземлення.

5) *Захист приміщень за допомогою особливого дизайну*. Мова йде про те, що в деяких випадках доцільне створювати особливий дизайн кімнати і розміщення в ній обладнання, щоб гарантувати, що ніяка інформація не може вислизнути.

6) *Застосування спеціальних програмних засобів*. Для захисту системи є спеціальні драйвера екрану, якій може відображати конфіденційну інформацію за допомогою шрифтів, які мінімізують енергію цих викидів. Використання текстових шрифтів із згладженими краями обмежить високочастотне випромінювання - випромінювання, яке випромінюється від комп'ютера.

Компанії і приватні особи можуть набувати комп'ютери, які сертифіковані TEMPEST, але висока вартість такої безпечної системи може виявитися непомірно високою для більшості споживачі. Для людей, які хочуть бути більш захищеними від TEMPEST, але не можуть інвестувати в обладнання такого рівня, є кілька простих кроків, які необхідно зробити, щоб зменшити компрометуючі випромінювання:

1) Придбайте комп'ютерне обладнання, яке відповідає сучасним нормам випромінювання.

2) Використовуйте тільки екранований кабель для всіх з'єднань системи, а кабель між компонентами повинен бути якомога коротшим.

3) Блокуйте випромінювання шнурів живлення з проводки будівлі за допомогою спеціальних фільтрів.

4) Для запобігання використанню телефонної, факсимільної або модемної лінії в якості антени, встановіть фільтр телефонної лінії.

5) З боку програмного забезпечення також рекомендується зашифрувати будь-які дані, які ви відправляєте зі свого комп'ютера. .

Системи захисту від TEMPEST-технології постійно удосконалюються. Результати можна знайти в різноманітних керівництвах з безпеки щодо випромінювання, що компрометують.

Висновки

Таким чином, вирішення проблеми TEMPEST - ненавмисного випромінювання електронного обладнання під час розвитку обчислювальної техніки є сьогодні актуальною. Треба враховувати, що поняття TEMPEST – це назва технології, що включає різні методи аналізу електромагнітного компрометуючого випромінювання таким чином, щоб їх можна було використовувати для відновлення перехоплених даних, які можуть мати компрометуючу інформацію.

Виконаний аналіз обладнання TEMPEST дозволяє стверджувати, що це обладнання включає в себе різні типи чутливих приймачів, які можуть контролювати широкий діапазон частот, а також комбінацію апаратного і програмного забезпечення, здатну обробляти отримані сигнали. Аналіз різних видів TEMPEST-технології, а саме: Tempest-атака, Soft TEMPEST, а також різновиди технологій перехоплення інформації шляхом прийому паразитного випромінювання сигналу монітора, пошуку необхідної інформації на диску, виведення інформації в незадіяний послідовний порт; відображення світлового потоку від екрану монітора на стінах; моделювання світлового потоку в світлодіодних індикаторах; під час випромінювання елементами комп'ютера; під час модулювання струму в комп‘ютері мовною інформацією; під час геолокації комп‘ютера; під час випромінювань в шинах комп‘ютері або кабелях внутрішнього з‘єднання; під час випромінювань в кабелях структурованої кабельної мережі внутрішнього з‘єднання в приміщенні.

Даються рекомендації щодо захисту від TEMPEST технологій для компаній і приватних осіб, а саме: мінімізація витоку електромагнітних випромінювань; екранування приміщень; екранування кабелів та окремих схем з конструкції обчислювальної техніки; заземлення корпусів обчислювальної техніки; захист приміщень за допомогою особливого дизайну; застосування спеціальних програмних засобів.

Список використаної літератури

1. Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286

2. Peter Wright: Spycatcher - The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Australia, 1987, ISBN 0-85561-098-0

3. Peter Smulders: The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security 9 (1990) 53-58

4. Markus G. Kuhn and Ross J. Anderson: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. University of Cambridge, Computer Laboratory, New Museums Site, Pembroke Street, Cambridge CB2 3QG, United Kingdom

5. Electromagnetic Pulse (EMP) and Tempest Protection for Facilities. Engineer Pamphlet EP 1110-3-2, 469 pages, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31, 1990

6. Deborah Russell, G. T. Gangemi Sr.: Computer Security Basics. Chapter 10: TEMPEST, O'Reilly & Associates, 1991, ISBN 0-937175-71-4

7. A. J. Mauriello: Join a government program to unveil Tempest-spec mysteries. EDN vol 28 no 13, pp 191–195, June 23, 1983

8. Комп'ютери в захищеному виконанні/[Електронний ресурс]. – Режим доступу: https://infopedia.su/1x979a.html

9. Програмні закладки/[Електронний ресурс]. – Режим доступу: http://um.co.ua/2/2-15/2-150885.html

Автори статті

Катков Юрій Ігорович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Бєлих Євген Юрійович – студент, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Katkov Yuriy Igorovich – candidate of Sciences (technical), associate professor of the Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Belykh Yevhen Yuriyovych – student, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 01.12.2020 р. Рецензент: д.т.н., доцент А.О. Макаренко