управления информационной безопасности организации. Отображено аспекты, связанные з персоналам и их обхождением с документами, касательно информационной безопасности предприятий и/или организаций.

Ключевые слова: документация, международные стандарты, системы управления, управление организацией, персонал.

YULIYA KOZHEDUB

CREATE DOCUMENTATION FOR INFORMATION SECURITY MANAGEMENT SYSTEMS

A new system for creating documentation for information security management systems, reflecting the peculiarities inherent in information security management system of the organization. Showing aspects of personnel and their handling of documents related to information security companies and / or organizations.

Keywords: documentation, international standards, system management, management organization, personnel.

Юлія Василівна Кожедуб, кандидат технічних наук, доцент, Державний заклад «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

E-mail : JuliaKozhedub@email.ua

Юлия Васильевна Кожедуб, кандидат технических наук, доцент, Государственное учреждение «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Yuliya Kozhedub, candidate of technical sciences, associate professor, State institution «Institute of special communication and information security of National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

УДК 004.056.5:621.39

ЮРИЙ ХЛАПОНИН

ВЫЯВЛЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВЕДЕНИЯ ПУТЕМ ОБРАБОТКИ ОБЛАСТИ СПЕКТРА СВЕРХВЫСОКИХ ЧАСТОТ

Проведен анализ образования канала утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН) для различных компонентов персонального компьютера (ПК). Для стандартного компьютерного монитора перехват информации возможен на частотах до 50 гармоники тактовой частоты. Излучение может происходить в широком диапазоне частот (от единиц Гц до ГГц), а дальность реального перехвата информации достигать сотен метров. Показано, что информативность сигналов ПЭМИН существенная на частотах единиц ГГц, и возникает вопрос о необходимости специальных исследований на частотах нескольких ГГц, хотя методика этого не требует.

Показано, что вопреки распространенному мнению заземление не играет определяющей роли в защите информации от утечки каналом ПЭМИН. Заземление необходимо только по требованиям электробезопасности. В некоторых случаях при

подключении заземления уровень побочных излучений может и увеличиться. Показано, что в большинстве практических случаев кабельная система – это отличная антенна для всех побочных излучений оборудования, подключенного к сети. Побочные излучения, возникающие в элементах компьютера, приводятся на все провода кабеля локальной сети.

Ключевые слова: информация, защита информации, побочные электромагнитные излучения и наводки, информативный сигнал.

Введение. Одним из возможных каналов утечки информации является излучение элементов компьютера, точнее, элементов основных технических средств (ОТС), если говорить о защищенных автоматизированных системах (АС). Принимая и декодируя эти излучения, можно получить сведения о всей информации, обрабатываемой в компьютере. Этот канал утечки информации называется ПЭМИН (побочного электромагнитного излучения и наводки). В Европе и Канаде применяется термин «compromising emanation» – компрометирующее излучения. В Америке применяется термин «TEMPEST» [1].

Частотный диапазон побочных электромагнитных излучений, простирается от единиц килогерц до гигагерц и выше и определяется тактовой частотой используемого средства обработки информации. Следует отметить, что ПЭМИН образуются от опасного сигнала. Опасный (информативный) сигнал – сигнал, который содержит, несет информацию в открытом виде [2].

Так, для стандартного компьютерного монитора перехват информации возможен на частотах вплоть до 50 гармоники тактовой частоты, а уровень излучения, составляет в ближней зоне величину до десятков дБ, позволяет принимать сигналы на расстоянии до нескольких сотен метров [3]. Кроме электромагнитных излучений вокруг средств обработки информации присутствуют квазистатические информационные электрические и магнитные поля, которые вызывают наводнения на близко расположенные кабели, телефонные провода, линии охранно-пожарной сигнализации, электросеть и т.п. Интенсивность полей в диапазоне частот от единиц килогерц до десятков мегагерц такова, что прием сигналов может вестись за пределами контролируемой зоны (КЗ) при непосредственном подключении к этим линиям передачи.

Исследование ПЭМИН элементов персональных электронно-вычислительных машин (ПЭВМ). Современные достижения в области технологии производства радиоприемных устройств позволяют создавать очень миниатюрные чувствительные приемники. Они могут находиться практически вплотную к объектам электронно-вычислительной техники (ЭВТ). В частности, в транспортных средствах или неконтролируемых «дипломатах» в течение всего рабочего времени, когда и осуществляется обработка большей части объемов информации с ограниченным доступом (ИсОД). Успешно внедряется многоканальный прием сигналов (как по различным направлениям, так и на разных частотах), с последующей их корреляционной обработкой. Это позволило значительно увеличить возможности перехвата информации.

На основании вышеизложенного обоснования и обеспечения необходимого в наше время уровня защищенности ИсОД от утечки по ПЭМИН и преднамеренного силового электромагнитного воздействия, объекты высших государственных органов, силовых и правоохранительных ведомств, отдельных центральных органов исполнительной власти и критических инфраструктур следует, по нашему мнению, считать размещёнными в, так сказать, «чрезвычайных условиях расположения» с точки зрения защиты информации.

Для обеспечения достаточного уровня защищенности ИсОД обработка такой информации должна осуществляться только ЭВМ в защищенном исполнении, которые отвечают действующим в Украине ГОСТ 29339-92.

Следует отличать термин «ЭВМ в защищенном исполнении» (в терминологии ГОСТ 29339-92 - по ПЭМИН) от выражения «защищенной ЭВМ» (дополнительными средствами, например от НСД, пространственным зашумлением или экранированием помещения).

ЭВМ в защищенном исполнении обеспечивает надежную защиту обрабатываемой информации от утечки ее по ПЭМИН, намеренного силового воздействия и от аппаратных закладок. В то же время использование систем пространственного зашумления лишь частично решает проблему защиты информации только от перехвата по ПЭМИН, не защищая совсем от намеренного силового воздействия и от аппаратных закладок [4]. Системы пространственного зашумления дополнительно повышают уровень электромагнитного излучения, создают помехи для РЭА, демаскируют местонахождения объекта и обработке ИсОД. Кроме того, не исключена возможность уменьшения или ликвидации совсем защитного действия генератора шума, например, пространственной селекцией направленными антеннами и современными методами обработки сигналов. Задача выделения информативного сигнала из смеси сигнал / помеха может быть значительно облегчена при условии предварительного определения характеристик информативных сигналов ЭВМ, перехваченных с демаскированного объекта в период отсутствия пространственного зашумления. Следует также заметить, что характеристики излучения информативных сигналов не зависят от степени секретности обрабатываемой информации.

Диапазон рабочих частот генераторов шума, которые предлагаются для маскировки информативных излучений, не превышает 1 ГГц, а утечка информации возможна и на более высоких частотах (до 10-15 гармоники тактовой частоты, на сегодня значительно превышает 1 ГГц).

Характер ПЭМИН определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также материалами, из которых изготовлен корпус, и его конструкция. Излучение может происходить в широком диапазоне частот (от единиц Гц до ГГц), а дальность реального перехвата информации достигать сотен метров.

Следует особо отметить, что применение на ПЭВМ, которая предназначена для обработки закрытой информации (то есть на ОТС), устройств, использующих любые беспроводные интерфейсы подключения (радиоканал, ИК-канал), кроме волоконно-оптических (ВОЛС), категорически запрещено. В связи с этим «радиоклавиатуры», мыши, ТВ-тюнеры и другую современную удобную периферию мы не рассматриваем принципиально. Протоколы IR Wave, 802.11 (с любыми индексами), BlueTooth, Wi-Fi, WiMAX и т.д. запрещены в принципе.

Излучение монитора – очень опасный канал утечки информации. Так, DVI интерфейс используется в настоящее время как в LCD мониторах, так и во многих типах телевизоров. Название разъема DVI происходит от английского сокращения Digital Visual Interface (цифровой видеоинтерфейс). Интерфейс DVI был разработан и внедрен в 1999 году организацией Digital Display Working Group (DDWG) и основан на формате последовательной передачи данных (PanelLink). Кабель DVI состоит из четырех витых пар красного, зеленого и синего цветов, а также и clock (сигнал тактовой частоты).

Перехват сигналов DVI вполне реален. Если полосу пропускания приемника иметь 200 МГц, тогда на частоте 1,2-2,5 ГГц, проанализировав 9-10 гармоники основной тактовой частоты интерфейса DVI (точнее – HDMI 1.3) можно реализовать перехват.

Существует общая методика исследования периодических негармонических сигналов (входных воздействий и их реакций) в электрической цепи, которая основана на разложении сигнала в ряд Фурье. Данная методика заключается в том, что всегда можно подобрать ряд гармонических (т.е. синусоидальных) сигналов с такими амплитудами, частотами и начальными фазами, алгебраическая сумма ординат которых в любой момент времени равна ординате исследуемого несинусоидального сигнала. По отзывам практиков, ПЭМИН можно выявить, проанализировав 5-9 гармонику сигнала на частоте выше 4 ГГц. Согласно же существующим методикам поиск излучения, модулированного тестовым сигналом осуществляется в диапазоне частот от 0,01 до 1000 МГц. В то же время тактовая частота компонентов компьютера может составлять единицы ГГц. Например, жесткие накопители с интерфейсом HDD SATA – 1500MHz, HDD SATA2 – 3000 MHz, HDD SATA – 600-+4800 MHz.

Исследование уровней излучения, создаваемых компьютерами в разных корпусах, серийно выпускаемых показали, что современные корпуса позволяют значительно ослабить излучение элементов компьютера. Однако качество экранирования корпуса системного блока компьютера влияет на уровень излучения всех устройств, подключенных к системному блоку. Например, клавиатура и монитор имеют достаточно высокий уровень излучения, и считается, что высокий уровень излучений определяется наличием в них соединительных кабелей. Это действительно так, однако в серийных корпусах компьютеров не нормируется ослабление электромагнитного поля. Поэтому одна и та же клавиатура или комплект «видеокарта – монитор – кабель» в разных корпусах могут иметь непредсказуемо разный уровень излучений. В частности, на рис. 1 и рис. 2 приведены уровни электрической составляющей информативных сигналов клавиатуры и монитора соответственно. Данные, обозначенные как E1, E2 и E3, относятся к трем разным серийным корпусам [5].

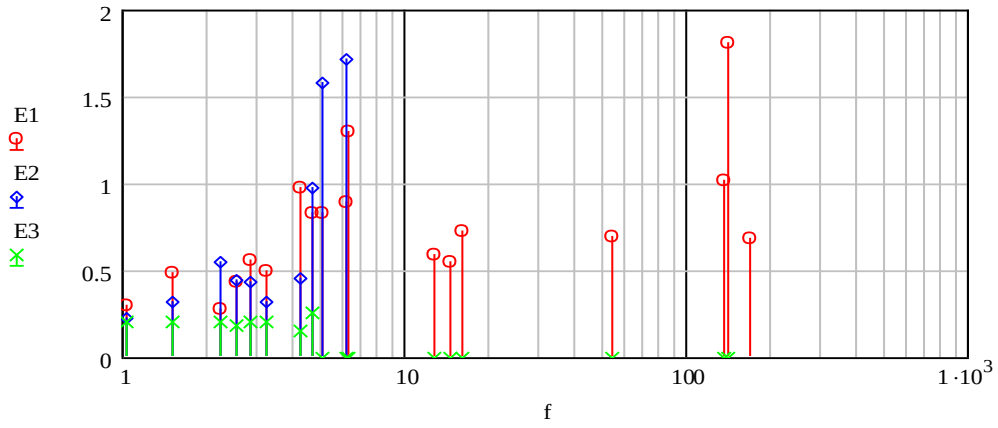

Рисунок 1 – Уровни электрической составляющей в режиме тестирования клавиатуры

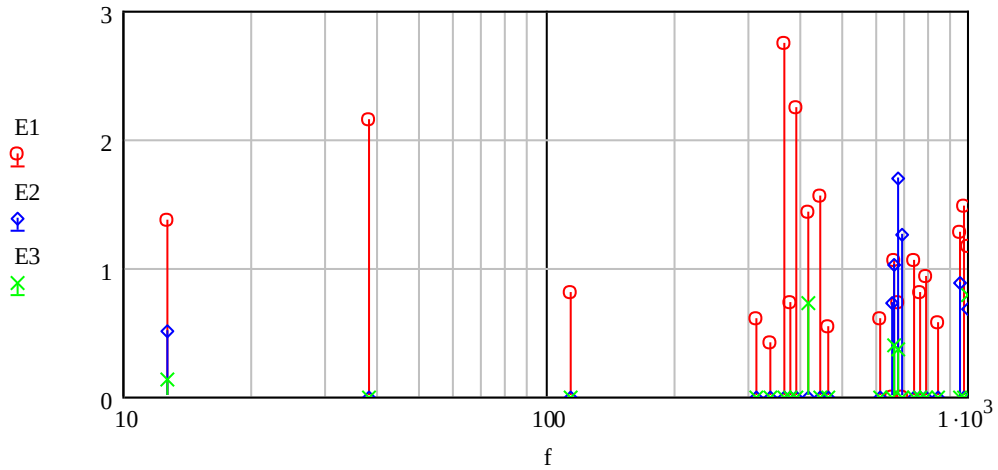

Рисунок 2 – Уровни электрической составляющей в режиме тестирования монитора

Из рис. 2 можно сделать вывод, информативность сигналов ПЭМИН существенная на грани 1 ГГц, и возникает вопрос о необходимости специальных исследований на частотах нескольких ГГц, хотя методика этого не требует.

Аналогичные соотношения получаются для всех устройств, входящих в состав ПК.

Наличие и качество заземления технических средств. Для автономных устройств ЭВТ, вопреки распространенному мнению заземление не играет определяющей роли в защите информации от утечки каналом ПЭМИН. Заземление необходимо только по требованиям электробезопасности [6].

Впрочем, через неидеальное экранирование определенное влияние заземления все же делает. Как правило, уровень побочных излучений при грамотно выполненном заземлении несколько снижается. Однако, в некоторых случаях при подключении заземления уровень

побочных излучений может и увеличиться. Поэтому нельзя однозначно утверждать, что заземление необходимо с точки зрения защиты информации от утечки по каналу ПЭМИН. И более того, чем качественнее выполнено экранирование корпуса (включая и качество фильтров в цепях электропитания), тем меньше сказывается на уровне побочных излучений наличие или отсутствие заземления.

Разделительный трансформатор предлагают [7] применять также для защиты объектов ЭВТ от помех в двухпроводной сети электропитания при отсутствии третьего защитного провода. Включение трансформатора и заземления корпуса компьютера, устраняет передачу опасных скачков напряжения помех с нулевого провода электросети на металлический корпус компьютера. Естественно, эта защита является эффективным на сравнительно низких частотах. Отдельный провод заземления – это и отдельный канал распространения и переизлучения высокочастотных сигналов, порожденных электромагнитным полем данного компьютера. Этот сигнал распространяется в линии, образованной проводами электропитания (включающие и металлический корпус фильтра) и обратным проводом, образованным землей или металлоконструкциями здания. Размеры эквивалентной линии или антенны – десятки метров, ее высота – единицы метров, поэтому эффективное переизлучение будет наблюдаться уже с частот порядка 1 МГц. Закрытие проводов заземления металлической трубой только увеличивает эффективную длину антенны (антенна Айзенберга [8]) и на высоких частотах не обеспечивает хорошего экранирования.

Побочные излучения кабельной системы (сети). Кабельная сеть не содержит активных и нелинейных элементов, поэтому сама по себе она не может быть источником побочных излучений. Однако кабельная сеть связывает между собой все элементы компьютерной сети. По ней передаются сетевые данные, но вместе с этим она также есть приемником всех наводок и средой для переноса побочных электромагнитных излучений.

Довольно часто при оценке защищенности кабельной системы интересуются только тем, насколько ослабляется побочное излучение, вызванное сигналами, которые передаются по кабелю в процессе сетевого обмена информацией. Но в большинстве практических случаев кабельная система – это отличная антенна для всех побочных излучений оборудования, подключенного к сети. Побочные излучения, возникающие в элементах компьютера, наводятся на все провода кабеля локальной сети. Поставить для этих проводов фильтр, подавляющий побочные излучения, невозможно. Ведь побочные излучения элементов компьютера (жесткий диск, клавиатура и т.д.) сосредоточены в той же полосе частот, что и спектр импульсов, передаваемых по витой паре в процессе сетевого обмена. Подавляя побочные излучения, мы подавим и сетевой трафик. Таким образом, если компьютер с защитой информации включить в локальную сеть на неэкранированной витой паре, то провода неэкранированной витой пары, играя роль антенны, могут усилить напряженность поля, создаваемого, например, клавиатурой компьютера в десятки тысяч раз [7]. Поэтому неэкранированная витая пара не может применяться в локальной сети, в которой обрабатывается информация с ограниченным доступом.

Выводы. В данной статье рассмотрены особенности возникновения канала утечки информации, обрабатываемой основными техническими средствами, за счет побочного электромагнитного излучения и наводки. ПЭМИН можно выявить, проанализировав 5-9 гармонику сигнала на частоте выше 4 ГГц, хотя в настоящее время при специсследованиях ограничиваются частотами 1-2 ГГц. Показано, что заземление не играет определяющей роли в системах защиты информации от утечки каналом ПЭМИН. Показано, что кабельная система может быть отличной антенной для всех побочных излучений оборудования, подключенного к сети. Предложено объекты высших государственных органов, силовых и правоохранительных ведомств, отдельных центральных органов исполнительной власти и критических инфраструктур считать размещенными в «чрезвычайных условиях расположения» с точки зрения защиты информации и для обеспечения достаточного уровня защищенности ИсОД обработка такой информации должна осуществляться только ЭВМ в защищенном исполнении, которые отвечают действующим в Украине ГОСТ 29339-92.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Kuhn G. Markus. Soft Tempest : Hidden Data Transmission Using Electromagnetic Emanations / Markus G. Kuhn, Ross J. Anderson // Lecture Notes in Computer Science. – 1998. – Vol. 1525. – P. 124-142.

2. Ленков С.В. Методы и средства защиты информации. Том I. Несанкционированное получение информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В.А. Хорошка. – К. : Арий, 2010. – 464 с.

3. Пятачков А. Г. Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам / А. Г. Пятачков. – М. : НП РЦИБ «Факел», 2007. – 194 с.

4. Левченко Г. Особливості використання ЕОМ для обробки інформації з обмеженим доступом в сучасних умовах / Г. Левченко, М. Ільченко, В. Хорошко, В. Буркацький, К. Золотухін, В. Грошев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2000. – Вип. 1 (1). – С. 84-87.

5. Чеховский С. Побочные излучения и защита информации в локальных сетях / С. Чеховский, Ю. Рудаков. – Режим доступа : http://www.epos.ua/view.php/pubs_2?subaction=showfull&id=1049662800&archive=&start_from=&ucat=2&. – Дата доступа : июль 2015. – Название с экрана.

6. Электроустановки зданий. Часть 7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации (IEC 60364-7-707-84) : ГОСТ Р 50571.22-2000 – [Действует с 2002-01-01]. – М. : Госстандарт России, 2000. – 8 с.

7. Стеченко В. Анализ защиты компьютера от утечки по цепям питания и заземления / В. Стеченко, В. Найденко, М. Прокофьев, А. Курашкевич / Правове, нормативне та метрологічне забезпечення системи захисту інформації в україні. 2007. – Вип. 1 (14). – С. 160-165.

8. Айзенберг Г. З. Коротковолновые антенны / [Г. З. Айзенберг, С. П. Белоусов, Э. М. Журбенко, Г. А. Клигер, А. Г. Курашов]; под ред. Г. З. Айзенберга. – М. : Радио и связь, 1985. – 536 с.

Статья поступила в редакцию 13.10.2015.

REFERENCE

1. Kuhn, G. Markus, Anderson, J. Ross (1998), *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, Lecture Notes in Computer Science, Vol. 1525, pp. 124-142.

2. Lenkov, S.V., Peregudov, D.A., Horoshko, V.A. (2010), *Metody i sredstva zashchity informatcii. Tom I. Nesanktcionirovannoe poluchenie informatcii* [Methods and means of information protection], Ariy Publ., Kyiv, 464 p.

3. Piatachkov, A. G. (2007), *Zashchita informatcii, obrabatyvaemoi vychislitelnoi tekhnikoi, ot utechki po tekhnicheskim kanalam* [Protection of information processed by computer technology from leakage through technical channels], NP RTsIB «Fakel» Publ., 194 p.

4. Levchenko, H., Ilchenko, M., Khoroshko, V., Burkatskyi, V., Zolotukhin, K., Hroshev, V. (2000), *Osoblyvosti vykorystannia EOM dlia obrobky informatsii z obmezhenym dostupom v suchasnykh umovakh* [Features of the use of computers for processing classified information in modern], Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, No. 1 (1), pp. 84-87.

5. CHekhovskii, S., Rudakov, IU., *Pobochnye izlucheniia i zashchita informatcii v lokalnykh setiakh* [Spurious emissions and information protection in local networks], available at : http://www.epos.ua/view.php/pubs_2?subaction=showfull&id=1049662800&archive=&start_from=&ucat=2& (accessed 12 July 2015).

6. State Committee for Standardization (2000), GOST R 50571.22-2000, *Elektroustanovki zdanii. CHast 7. Trebovaniia k spetcialnym elektroustanovkam. Razdel 707. Zazemlenie oborudovaniia obrabotki informatcii* [Electrical installations of buildings. Part 7. Requirements for

specical installations or locations. Section 707. Earthing requirements for the installation of data processing equipment], Moskow, 8 p.

7. Stechenko, V., Naidenko, V., Prokofev, M., Kurashkevich, A. (2007), *Analiz zashchity kompiutera ot utechki po tcepiam pitaniia i zazemleniia* [Analysis of computer protection against leakage through the supply lines and ground], Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, No. 1 (14), pp. 160-165.

8. *Aizenberg, G. Z., Belousov, S. P., ZHurbenko, E. M., Kliger, G. A., Kurashov, A. G.(1985), Korotkovolnovye antenny* [Shortwave antenna], Radio i svyaz Publ., Moskow, 536 p.

ЮРІЙ ХЛАПОНІН

ВИЯВЛЕННЯ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ І НАВЕДЕННЬ ШЛЯХОМ ОБРОБЛЕННЯ ОБЛАСТІ СПЕКТРУ НАДВИСОКИХ ЧАСТОТ

Проведено аналіз утворення каналу витоку інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН) для різних компонентів персонального комп'ютера. Для стандартного комп'ютерного монітора перехоплення інформації можливе на частотах до 50 гармоніки тактової частоти. Випромінювання може відбуватися в широкому діапазоні частот (від одиниць Гц до ГГц), а дальність реального перехоплення інформації досягати сотень метрів. Показано, що інформативність сигналів ПЕМВН істотна на частотах одиниць ГГц, і виникає питання про необхідність спеціальних досліджень на частотах декількох ГГц, хоча методика цього не вимагає.

Показано, що всупереч поширеній думці заземлення не відіграє визначальної ролі в захисті інформації від витоку каналом ПЕМВН. Заземлення необхідне тільки за вимогами електробезпеки. У деяких випадках при підключенні заземлення рівень побічних випромінювань може і збільшитися. Показано, що в більшості практичних випадків кабельна система – це відмінна антена для всіх побічних випромінювань обладнання, підключеного до мережі. Побічні випромінювання, що виникають в елементах комп'ютера, наводяться на всі дроти кабелю локальної мережі.

Ключові слова: інформація, захист інформації, побічні електромагнітні випромінювання і наведення, інформативний сигнал.

YURII KHLAPONIN

REVEALING CHANNELS OF INFORMATION LEAKAGE DUE TO STRAY ELECTROMAGNETIC RADIATION AND GUIDANCE BY TREATING THE SPECTRUM MICROWAVE FREQUENCY

The analysis of the formation of information leakage through electromagnetic radiation and side are different components of a PC. For a standard computer monitor interception is possible at frequencies up to 50 harmonics of the clock frequency. Emission can occur over a wide range of frequencies (from several Hz to GHz) and the range of real interception reach hundreds of meters. It is shown that the information content of signals is significant at frequencies GHz TEMPEST units, and there is the need for special studies at frequencies of several GHz, although the method does not require it.

It is shown that, contrary to popular belief grounding does not play a determining role in the protection of information from leakage channel TEMPEST. Grounding is only necessary for the requirements of electrical safety. In some cases, when you connect the ground level of spurious emissions may increase. It is shown that, in most practical cases, the cable system is a great dish for all spurious equipment connected to the network. Spurious emissions arising in the components of the computer are directed on all the wires of the cable network.

Keywords: information, information protection, side electromagnetic radiation and crosstalk, informative signal.

Юрий Иванович Хлапонин, кандидат технических наук, старший научный сотрудник, доцент, кафедра средств защиты информации, Национальный авиационный университет, Киев, Украина.
E-mail: yfcnz0408@ukr.net.

Юрій Іванович Хлапонін, кандидат технічних наук, старший науковий співробітник, доцент, кафедра засобів захисту інформації, Національний авіаційний університет, Київ, Україна.

Yurii Khlaponin, candidate of technical sciences, senior researcher, associate professor, academic department of information security tools, National Aviation University, Kyiv, Ukraine.