ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

ПРЕДНАМЕРЕННЫЕ ЭЛЕКТРОМАГНИТНЫЕ ВОЗДЕЙСТВИЯ ОТ БЛОКИРОВАНИЯ ДОСТУПА К ИНФОРМАЦИИ ДО СОЗДАНИЯ КАНАЛОВ УТЕЧКИ И УПРАВЛЕНИЯ

Агуреев Иван Александрович,
старший преподаватель кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Васильев Андрей Савельевич,
старший преподаватель кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Рыжиков Сергей Сергеевич,
доцент кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Пичугина Елена Анатольевна,
ассистент кафедры безопасности и информационных технологий, Национальный исследовательский университет "МЭИ", 111250, Россия, г. Москва, Красноказарменная улица, дом 14, e-mail: universe@mpei.ac.ru

Аннотация

Рассмотрены различные аспекты влияния внешних преднамеренных электромагнитных воздействий на информационные системы – от целенаправленных помех и нарушения функционирования средств до создания каналов утечки обрабатываемой информации и управления информационными процессами непосредственно в технических средствах.

Ключевые слова: преднамеренных электромагнитных воздействий, канал утечки информации, информационные системы.

INTENTIONAL ELECTROMAGNETIC INFLUENCES FROM BLOCKING ACCESS TO INFORMATION TO CREATING LEAKAGE AND CONTROL CHANNELS

Ivan A. Agureev,
senior lecturer of the Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

Andrey S. Vasilyev,
senior lecturer of the Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

Sergey S. Ryzhikov,
Associate Professor of the Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

Elena A. Pichugina,
Assistant, Department of Security and Information Technologies, National Research University "MPEI", 111250, Russia, Moscow, Krasnokazarmennaya street, building 14, e-mail: universe@mpei.ac.ru

ABSTRACT

Various aspects of the influence of external intentional electromagnetic influences on information systems are considered - from targeted interference and disruption of the functioning of equipment to the creation of leakage channels for processed information and management of information processes directly in technical equipment.

Keywords: intentional electromagnetic influences, information leakage channel, information systems.

Преднамеренные электромагнитные воздействия, направленные на блокирование доступа к информации

Современное общество в условиях цифровой трансформации экономики и всех сфер жизни тесно связано с получением, хранением, обработкой и использованием разнообразной информации, в том числе и ограниченного доступа. Наряду с угрозами нарушения конфиденциальности и целостности информации, особую актуальность приобретает угроза блокирования, когда законные пользователи сталкиваются с прекращением или затруднением доступа к информации [1].

Реализация данной угрозы может быть за счёт влияния на соответствующие информационные системы преднамеренными электромагнитными воздействиями (ПЭМВ), среди которых следует выделить целенаправленные электромагнитные помехи и преднамеренное силовое электромагнитное воздействие на информацию, которое, помимо её блокирования, может привести и к нарушению целостности.

Устройства, генерирующие преднамеренные электромагнитные воздействия в определенных частотных диапазонах, широко применяются при ведении радиоэлектронной борьбы (прицельные, заградительные и другие типы помех) [2-4]. Электромагнитной помехой (Electromagnetic interference) является нежелательное физическое явление или воздействие электрических, магнитных или электромагнитных полей, электрических токов или напряжений внешнего или внутреннего источника, которое нарушает нормальную работу технических средств и (или) вызывает ухудшение технических характеристик и параметров этих средств [5].

Под преднамеренным силовым электромагнитным воздействием на информацию следует понимать несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем [6].

Силовые ПЭМВ могут быть осуществлены открыто или скрытно (замаскированы под действие электромагнитных помех), дистанционным (по эфиру) или контактным (по сети) способом и направлены на достижение сбоя, нарушения нормального функционирования электронных систем (вплоть до разрушения отдельных элементов интегральных схем). Для создания данных ПЭМВ может применяться достаточно малогабаритное устройство, состоящее из первичного источника энергии (например, емкостной батареи), генератора (генератор с взрывной накачкой, генератор Маркса и пр.), быстродействующего переключающего элемента и направленной антенны (рис. 1).

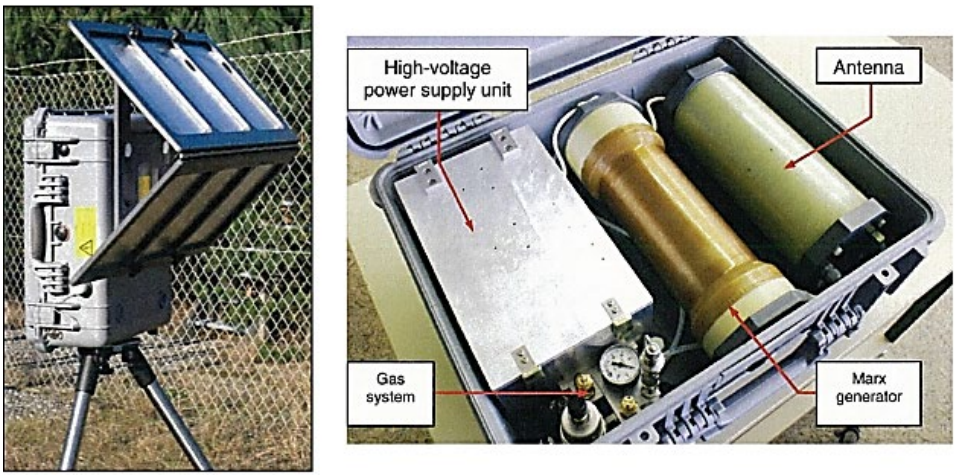

Рис. 1. Генератор DS 110, серийно выпускаемый кампанией Diehl BGT Defense GmbH & Co (Германия)

Технологические разработки в области создания силовых ПЭМВ позволили создать установки, способные генерировать сильные электромагнитные воздействия при достаточно компактных размерах (рис. 2).

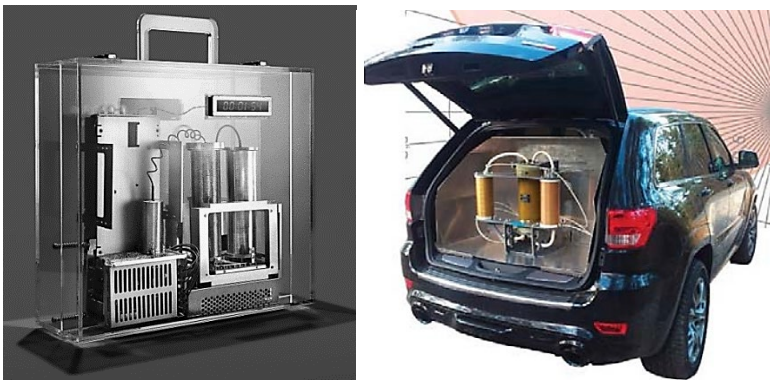

Рис. 2. Установки ПЭМВ, размещаемые в кейсе и багажнике автомобиля

Возможность атаки посредством генерации электромагнитного импульса на информационное оборудование, находящееся в зоне действия генератора ПЭМВ, может привести не только к временному нарушению работоспособности (сбои, зависание), но и к

разрушению внутренних цепей, что сделает его полностью непригодным для дальнейшей работы (рис. 3) [7].

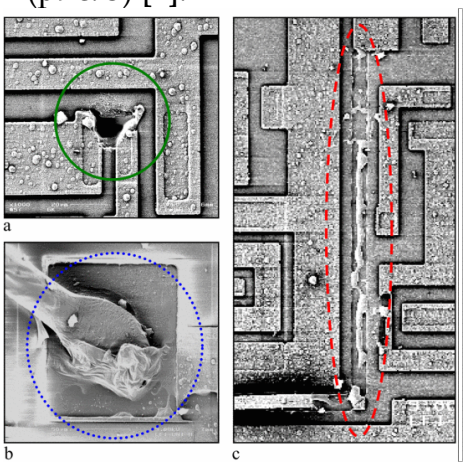

Рис. 3. Разрушение интегральных схем: а – пробой перехода; в – разрушение контактной площадки, с – оплавление проводника

Оценка восприимчивости различных ИТ-устройств к мощному электромагнитному импульсу содержится в [8].

Кроме деструктивных воздействий посредством направленных ПЭМВ относительно малой мощности возможно создание как технических каналов утечки информации из устройств ее обработки, так и каналов для внедрения внешних сигналов с целью управления информационными процессами, протекающими в атакуемом техническом средстве.

Преднамеренные электромагнитные воздействия, направленные на создание каналов утечки информации и управления информационными процессами

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала через физическую среду от его источника до технического средства, осуществляющего перехват информации [9].

Целью ПЭМВ в виде целенаправленного высокочастотного облучения (ВЧО) технического средства (ТС) является организация утечки внутренних информационных сигналов, путем воздействия радиоволной определенной частоты на заранее внедренную аппаратную закладку (рис. 4). Подобного рода атака обозначается аббревиатурой RFRA (Radio-frequency Retroreflector Attack) [10, 11].

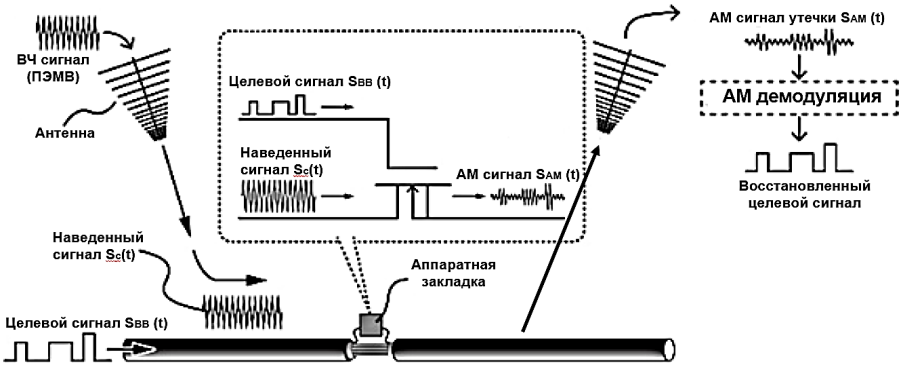

Рис. 4. Схема радиочастотной атаки с переотражением ВЧ сигнала

В результате высокочастотного преднамеренного электромагнитного воздействия определенной частоты на ТС, в которое заранее внедрена аппаратная закладка, в проводнике, выполняющем роль дипольной антенны, индуцируется сигнал SC(t). Полевой транзистор, выполняющий функцию аппаратной закладки, осуществляет модуляцию наведенного в кабеле сигнала SC(t) информационной последовательностью SBB(t), подаваемой на затвор транзистора. В результате в кабеле начинает протекать ток SAM(t), модулированный по величине целевым информационным сигналом SBB(t). Наведенный АМ-сигнал SAM(t) излучается дипольной антенной в эфир для дальнейшей АМ-демодуляции и восстановления исходного целевого сигнала.

Уровень переизлученного сигнала SAM(t) и, следовательно, дальность реализуемой атаки, пропорциональны интенсивности ПЭМВ, которое определяет величину наведенного сигнала SC(t). а также зависит от кратности совпадения частоты облучения и резонансной частоты непреднамеренной антенны. Резонансные частоты непреднамеренной антенны (кабеля, в который внедрена аппаратная закладка) определяются ее физической структурой, длиной и комплексным сопротивлением, что предопределяет необходимость изменения частоты облучения в определенных пределах, для достижения соотношения между длиной (d) проводника и частотой (длиной волны λ) ПЭМВ

$$d = \frac{(2n+1)\lambda}{2},$$

где n=0,1, 2, ..., λ.

С целью улучшения качества атаки для согласования параметров приемной антенны и частоты ПЭМВ в ТС возможна установка специальных ферритовых фильтров, которые в целом не влияют на работу ТС, но повышают избирательность антенны и делают ее более чувствительной к частоте облучения. В качестве таких элементов могут применяться ферритовые чипы Murata BLM18RK102SN1 (рис. 5), выпускаемые для установки в линии питания постоянного тока, в высокоскоростные сигнальные линии и др. [12].

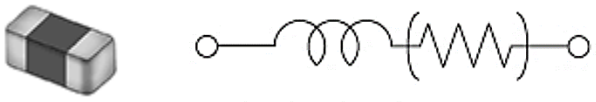

Рис. 5. Внешний вид и эквивалентная схема ферритового фильтра

Подобная доработка делает возможной реализацию не только канала утечки информации, обрабатываемой в ТС за счет ВЧО, но и формирование канала управления информационными процессами, путем воздействия на специально подготовленное средство модулированным ПЭМВ (рис. 6).

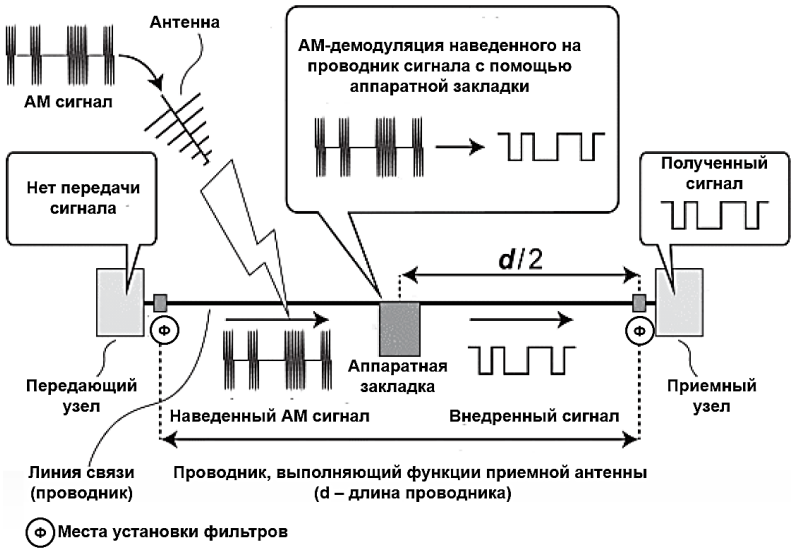

Рис. 6. Принцип внедрения в ТС внешнего сигнала

Более детально формирование канала управления информационными процессами, с рассмотрением варианта установки аппаратной закладки на базе полевого транзистора, внедренного вместе с ферритовыми фильтрами в экранированный связной кабель, приведена в [13].

Заключение

Спектр применения преднамеренных электромагнитных воздействий на информационные системы достаточно широк: от создания помех, направленных на блокирование доступа к информации и нарушения функционирования технических средств и систем путем разрушения внутренних цепей и связей, до формирования каналов утечки обрабатываемой информации и внедрения внешних сигналов, позволяющих влиять на информационные процессы. При этом реализация каналов утечки и управления возможна только при условии предварительного внедрения в атакуемое ТС элементов аппаратной закладки.

Частично нейтрализовать ПЭМВ (в части создания каналов утечки и управления) возможно за счет ослабления уровня воздействия путем экранирования ТС, замены медных кабелей, по возможности, на оптоволоконные, применения помехоустойчивых схемотехнических решений и проведения специальной проверки ТС на предмет выявления возможно внедренных элементов устройств негласного получения информации.

Список литературы:

1. ГОСТ Р 53113.1—2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 531-ст: дата введения 2009.01.10. – URL: https://docs.cntd.ru/document/1200075568.html (дата обращения: 02.02.2023). – Текст: электронный.
2. Перунов, Ю. М. Радиоэлектронная борьба в информационных каналах / Ю. М. Перунов, А. И. Куприянов. – Москва; Вологда: Инфра-Инженерия, 2021. – 452 с.: ил., табл., схем., граф. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=617263 (дата обращения: 02.02.2023). – Библиогр. в кн. – ISBN 978-5-9729-0718-2. – Текст: электронный.

3. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории / Куприянов А. И., Шустов Л. Н. - 3-е изд. - М.: Вузовская книга, 2017. - 798 с.: ил. - Библиогр.: с. 789-792. - ISBN 978-5-9502-0812-6.
4. Михайлов Р. Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоретический труд. – СПб.: Наукоемкие технологии, 2018. – 131 с.
5. Электромагнитная помеха // Википедия [2021]. Дата обновления: 29.07.2021. URL: https://ru.wikipedia.org/?curid=382791&oldid=115739385 (дата обращения: 02.02.2023).
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст: дата введения 2008-02-01. – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 02.02.2023). – Текст: электронный.
7. S. Korte, M. Camp and H. Garbe, "Hardware and software simulation of transient pulse impact on integrated circuits," 2005 International Symposium on Electromagnetic Compatibility, 2005. EMC 2005., Chicago, IL, USA, 2005, pp. 489-494 Vol. 2, doi: 10.1109/ISEMC.2005.1513564.
8. R. Przesmycki & M. Wnuk, "Susceptibility of IT devices to HPM pulse", International Journal of Safety and Security Engineering, Vol. 8, No. 2 (2018) 223–233, DOI: 10.2495/SAFE-V8-N2-223-233
9. Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. Приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст. - Введ. 2006-06-01. - М.: Стандартинформ, 2006. - 16 с.
10. Реализация канала утечки конфиденциальной информации за счет ВЧ облучения. Серия: Естественные и технические науки, №12, декабрь 2021 г., стр. 135-144. DOI 10.37882/2223–2966.2021.12.31
11. S. Kaji, D. Fujimoto, Y. Kim and Y. Hayashi, "A Fundamental Evaluation of EM Information Leakage Induced by IEMI for a Device with Differential Signaling," 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Nusa Dua - Bali, Indonesia, 2021, pp. 1-4, doi: 10.1109/APEMC49932.2021.9597081.
12. Reference Specification. EMI Suppression Filters/Ferrite Beads/Inductor type filters/Chip Ferrite Bead BLM18. URL: https://www.murata.com/en-global/search/productsearch?cate=cgsubChipFerriBead&partno=BLM18,BLM21&realtime=1&rows=50 (дата обращения: 016.02.2023).
13. S. Kaji, M. Kinugawa, D. Fujimoto and Y. -i. Hayashi, "Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1115-1121, Aug. 2019, doi: 10.1109/TEMC.2018.2849105.

References:

1. GOST R 53113.1—2008. Information technology. Protection of information technologies and automated systems from information security threats implemented using covert channels. Part 1. General provisions: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated December 18, 2008 No. 531-st: date of implementation 2009.01.10. – URL: https://docs.cntd.ru/document/1200075568.html (access date: 02/02/2023). – Text: electronic.
2. Perunov, Yu. M. Electronic warfare in information channels / Yu. M. Perunov, A. I. Kupriyanov. - Moscow; Vologda: Infra-Engineering, 2021. – 452 pp.: ill., table, diagrams, graph. – Access mode: by subscription. – URL: https://biblioclub.ru/index.php?page=book&id=617263 (access date: 02/02/2023). – Bibliography in the book – ISBN 978-5-9729-0718-2. – Text: electronic.
3. Kupriyanov A.I., Shustov L.N. Electronic warfare. Fundamentals of theory / Kupriyanov A.I., Shustov L.N. - 3rd ed. - M.: University Book, 2017. - 798 p.: ill. - Bibliography: p. 789-792. - ISBN 978-5-9502-0812-6.
4. Mikhailov R. L. Electronic warfare in the US Armed Forces: military theoretical work. – St. Petersburg: Science-intensive technologies, 2018. – 131 p.
5. Electromagnetic interference // Wikipedia [2021]. Update date: 07/29/2021. URL: https://ru.wikipedia.org/?curid=382791&oldid=115739385 (access date: 02/02/2023).
6. GOST R 50922-2006. Data protection. Basic terms and definitions: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated December 27, 2006 N 373-st: implementation date 2008-02-01. – URL: https://docs.cntd.ru/document/1200058320 (date of access: 02.02.2023). – Text: electronic.
7. S. Korte, M. Camp and H. Garbe, "Hardware and software simulation of transient pulse impact on integrated circuits," 2005 International Symposium on Electromagnetic Compatibility, 2005. EMC 2005., Chicago, IL, USA, 2005, pp . 489-494 Vol. 2, doi: 10.1109/ISEMC.2005.1513564.
8. R. Przesmycki & M. Wnuk, "Susceptibility of IT devices to HPM pulse", International Journal of Safety and Security Engineering, Vol. 8, No. 2 (2018) 223–233, DOI: 10.2495/SAFE-V8-N2-223-233
9. Technical protection of information. Basic terms and definitions: recommendations for standardization R 50.1.056-2005: approved. By Order of Rostechregulirovanie dated December 29, 2005 No. 479-st. - Enter. 2006-06-01. - M.: Standartinform, 2006. - 16 p.
10. Implementation of a channel for leaking confidential information due to HF radiation. Series: Natural and Technical Sciences, No. 12, December 2021, pp. 135-144. DOI 10.37882/2223–2966.2021.12.31
11. S. Kaji, D. Fujimoto, Y. Kim and Y. Hayashi, "A Fundamental Evaluation of EM Information Leakage Induced by IEMI for a Device with Differential Signaling," 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), Nusa Dua - Bali, Indonesia, 2021, pp. 1-4, doi: 10.1109/APEMC49932.2021.9597081.
12. Reference Specification. EMI Suppression Filters/Ferrite Beads/Inductor type filters/Chip Ferrite Bead BLM18. URL: https://www.murata.com/en-

global/search/productsearch?cate=cgsubChipFerriBead&partno=BLM18,BLM21&realtime=1&rows=50 (access date: 02/016/2023).

13. S. Kaji, M. Kinugawa, D. Fujimoto and Y. -i. Hayashi, “Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan,” in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1115-1121, Aug. 2019, doi: 10.1109/TEMC.2018.2849105.