DOI 10.37882/2223–2966.2021.12.31

РЕАЛИЗАЦИЯ КАНАЛА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ЗА СЧЕТ ВЧ ОБЛУЧЕНИЯ

IMPLEMENTATION OF CONFIDENTIAL INFORMATION LEAKAGE CHANNEL DUE TO HF IRRADIATION

S. Smirnov
S. Ryzhikov
I. Agureev

Summary. The article discusses the options for the implementation of channels of leakage of confidential information from technical means by organizing an active attack, providing for their high-frequency irradiation. The purpose of this work is to show the feasibility of this approach and to assess the conditions for carrying out an attack.

Keywords: channel of confidential information leakage, high-frequency irradiation, modulator, reflected signal.

Смирнов Сергей Николаевич
Д.т.н., профессор, МГТУ имени Н.Э. Баумана
smirnovsn@bmstu.ru
Рыжиков Сергей Сергеевич
К.т.н., с.н.с., доцент, НИУ «МЭИ»
ryzhikovss@mpei.ru
Агуреев Иван Александрович
НИУ «МЭИ»
agureev.ivan@list.ru

Аннотация. В статье рассмотрены варианты реализации каналов утечки конфиденциальной информации из различных технических средств путем организации активной атаки, предусматривающей их высокочастотное облучение. Цель данной работы — показать реализуемость данного подхода и оценить условия осуществления атаки.

Ключевые слова: канал утечки конфиденциальной информации, высокочастотное облучение, модулятор, отраженный сигнал.

Введение

В связи с нарастающим переходом во всех сферах деятельности к электронному документообороту все больше конфиденциальной информации (КИ) обрабатывается в цифровом виде различными техническими средствами (ТС). При обработке информации в ТС неизменно образуется побочное электромагнитное излучение (ПЭМИ), перехват которого злоумышленником делает возможным раскрытие КИ без прямого доступа к обрабатывающему устройству.

Перехват ПЭМИ следует рассматривать как пассивную атаку, выполняемую путем приема и последующей обработки параметров электромагнитного излучения, исходящего от целевого устройства. Впечатляющие результаты возможности восстановления изображения за счет перехвата излучений от планшета представлены в [1].

Еще один риск утечки КИ связан с возможными активными атаками ТС, на которые воздействуют внешним электромагнитным излучением, т.е. за счет высокочастотного облучения (ВЧО). Необходимым условием успешной реализации подобных атак является наличие в атакуемом ТС заранее внедренной схемы — радиочастотного отражателя-модулятора (РОМ). В иностранной литературе данная атака обозначается аббревиатурой — RFRA (Radio-frequency Retroreflector Attack).

Реализация активной атаки

Сценарии установки РОМ в технические средства рассмотрены в [2]. Вместо специальной антенны могут использоваться защитные оплетки кабеля, соединительные кабели, печатные проводники, которые исполняют роль непреднамеренной приемо-передающей антенны. В [2, 5, 6] в качестве РОМ рассматривается (рис. 1) сборка на основе полевого транзистора, который нагружен на кабель (как вариант на печатные проводники), используемый в качестве дипольной антенны.

Принцип утечки информации с использованием РОМ представлен на рис. 2. Атакующий облучает ТС, в которое внедрен РОМ, высокочастотным излучением определенной частоты, которая индуцирует в кабеле, выполняющем роль дипольной антенны, сигнал $S_C(t)$.

Полевой транзистор осуществляет модуляцию наведенного в кабеле сигнала $S_C(t)$ информационной последовательностью $S_{BB}(t)$, подаваемой на затвор транзистора. В результате в кабеле начинает протекать ток $S_{AM}(t)$, модулированный по величине целевым информа-

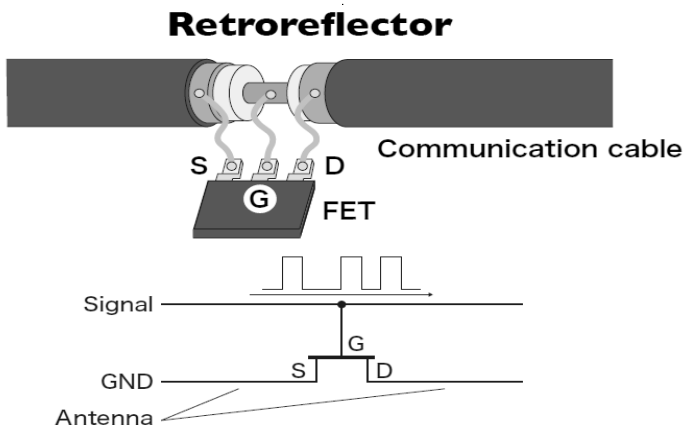

Рис. 1. Вариант применения полевого транзистора в качестве модулятора

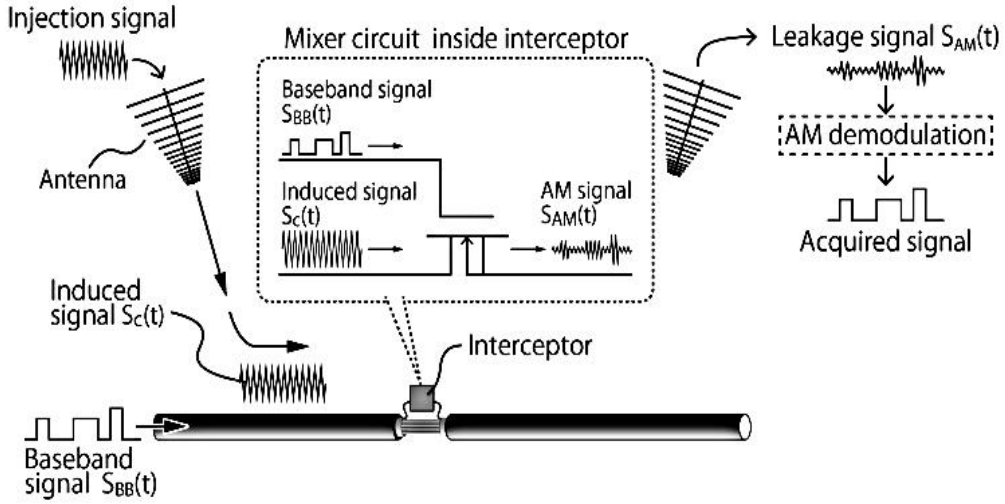

Рис. 2. Принцип утечки информации с использованием РОМ

ционным сигналом $S_{BB}(t)$. Наведенный АМ сигнал $S_{AM}(t)$ излучается дипольной антенной в эфир. Атакующий демодулирует принятый сигнал АМ и восстанавливает исходный целевой сигнал.

Уровень переизлученного сигнала $S_{AM}(t)$ и, следовательно, дальность реализуемой атаки, пропорциональна интенсивности внешнего электромагнитного облучения, которое определяет величину наведенного сигнала $S_C(t)$, а также кратностью совпадения частоты облучения и резонансной частоты непреднамеренной антенны. Резонансные частоты непреднамеренной антенны определяются ее физической структурой, длиной и комплексным сопротивлением.

Следовательно, дальность атаки может быть увеличена путем соблюдения вышеуказанных факторов в пределах рабочего диапазона полевого транзистора, на котором реализован РОМ.

1. Активная атака на VGA-монитор

Кабель VGA и монитор являются типичными средами для передачи и вывода информации в компьютерной системе. Большинство современных мониторов используют метод генерации видеоизображения с помощью построчной развертки. Яркости пикселей в линии развертки являются функциями напряжения графического сигнала. Любой цвет представляет собой визуальную смесь различных уровней яркости 3 основных цветов RGB.

Для работы с текстовыми документами используются два цвета: черный (текст) и белый (фон). Черный и белый

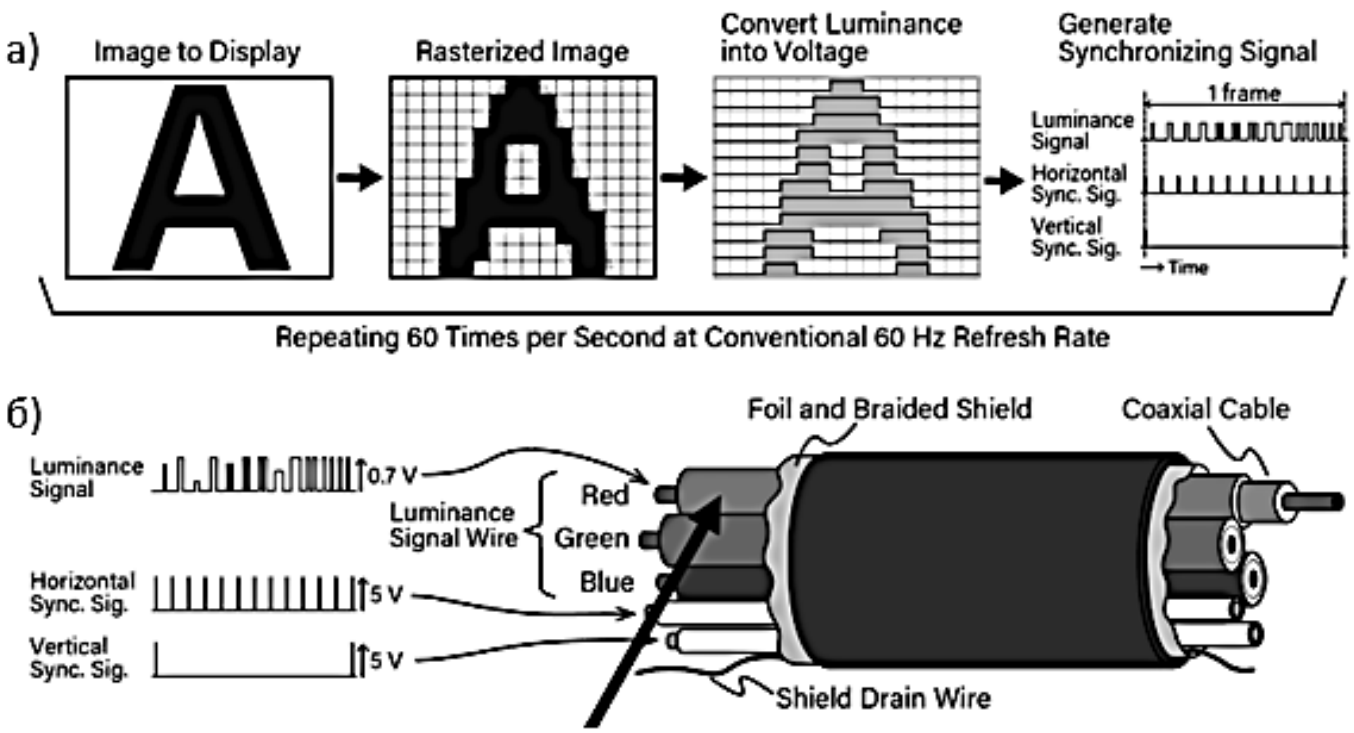

Рис. 3. Организация трансляции сигналов по VGA кабелю

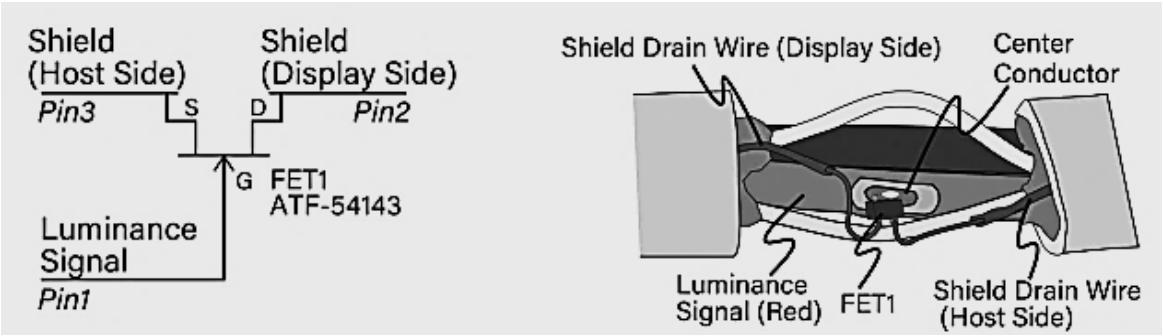

Рис. 4. Схема реализации РОМ и схема подключения на канал управления красным цветом

Рис. 5. Возможное место установки РОМ

Рис. 6. Восстановленное изображение с экрана монитора

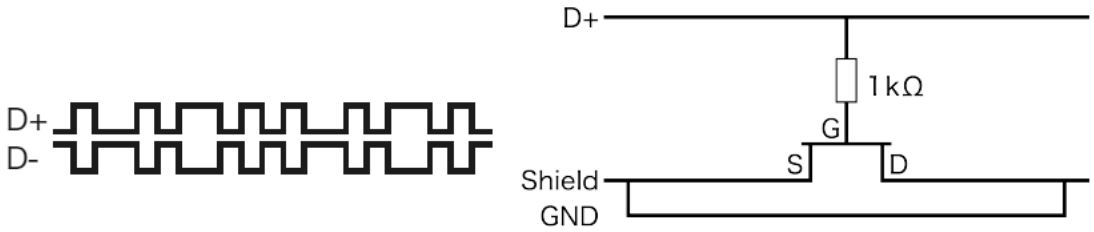

Рис. 7. 1-й вариант подключения РОМ в USB-кабель

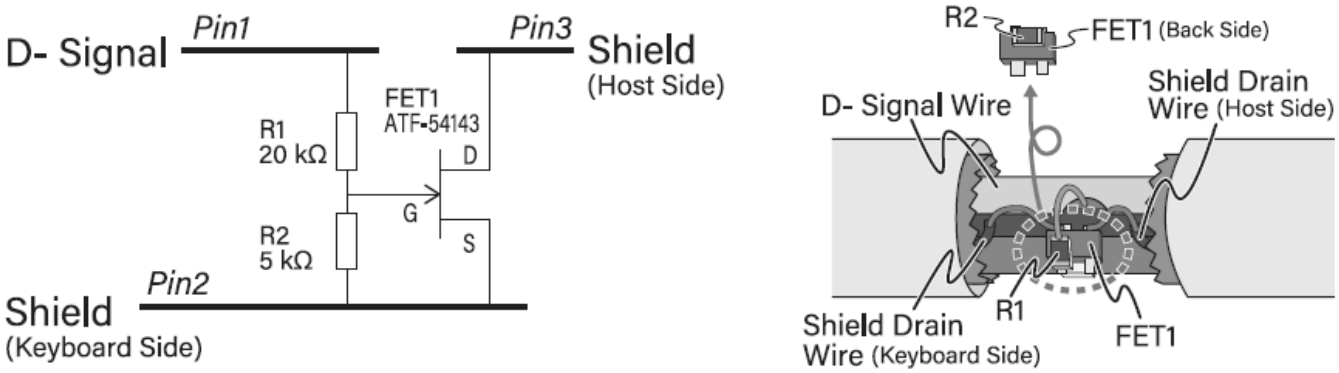

Рис. 8. 2-й вариант подключения РОМ в USB-кабель

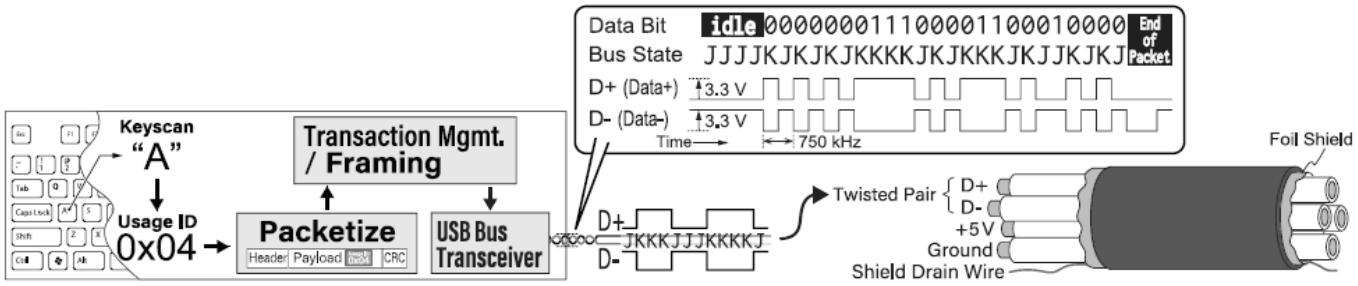

Рис. 9. Сигналы связи клавиатуры USB

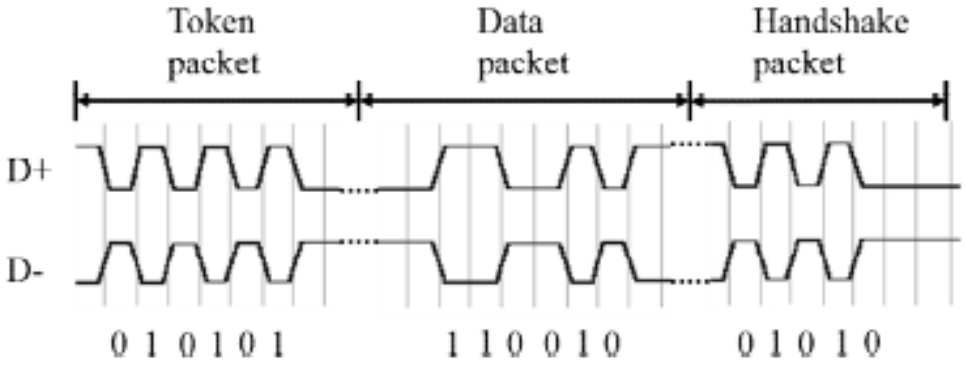

Рис. 10. Протокол USB-клавиатуры

цвета на экране монитора образуются следующими комбинациями: Black = 0+0+0 и White = R_{max}+ G_{max}+ B_{max}. Таким образом, получить информацию, отображаемую на экране, возможно реализуя перехват только одного сигнала, например, красного (рис. 3). Сигнал горизонтальной синхронизации HSYNC и сигнал вертикальной синхронизации VSYNC имеют свои каналы управления в кабеле VGA (рис. 3б), и они не передаются с цветным сигналом.

Отсутствие синхронизации может привести к визуальным артефактам в восстановленном изображении, включая повторение (из-за вертикальной синхронизации) и разрыв (из-за горизонтальной синхронизации). Тем не менее, можно восстановить сигнал горизонтальной синхронизации и сигнал вертикальной синхронизации из канала управления цветом, используя определенные алгоритмы синхронизации [7, 8].

Принципиальная схема РОМ и схема подключения на канал управления красным цветом для аналогового видеосигнала RGB на кабеле VGA показаны на рис. 4, а одно из возможных мест установки — на рис. 5. [2, 9]

Контакт Pin1 (рис. 4) подключен к проводнику коаксиального кабеля, который передает красный сигнал яркости, контакт Pin2 подключен к защитному экрану кабеля VGA в сторону дисплея, а контакт Pin3 — к защитному экрану в сторону ПК. Амплитудно-модулированные сигналы утечки об информации в канале управления красным цветом генерируются путем умножения высокочастотных сигналов, наведенных между контактами Pin2 и Pin3 за счет ВЧО, на сигнал изменения яркости в красном канале (Pin1). Кабель VGA в данном случае выступает непреднамеренной дипольной антенной. С помощью АМ-демодуляции принятого переотраженного сигнала можно получить информацию об изменении яркости в канале управления красным цветом и восстановить изображение, транслируемое на экран атакуемого монитора.

Восстановленное изображение, полученное в результате атаки с расстояния 5 м, представлено на рис. 6. [2]

2. Активная атака на USB-клавиатуру

Кабель USB содержит четыре экранированных провода: VBUS (питание), GND (земля), D+ и D-(сигнальные линии для передачи дифференциальных, т.е. в противофазе, сигналов). Дифференциальная передача сиг-

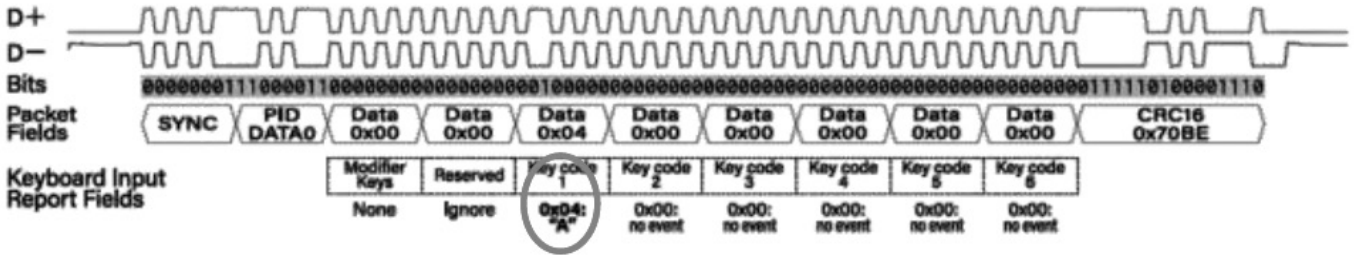

Рис. 11. Пакетный формат USB-клавиатуры

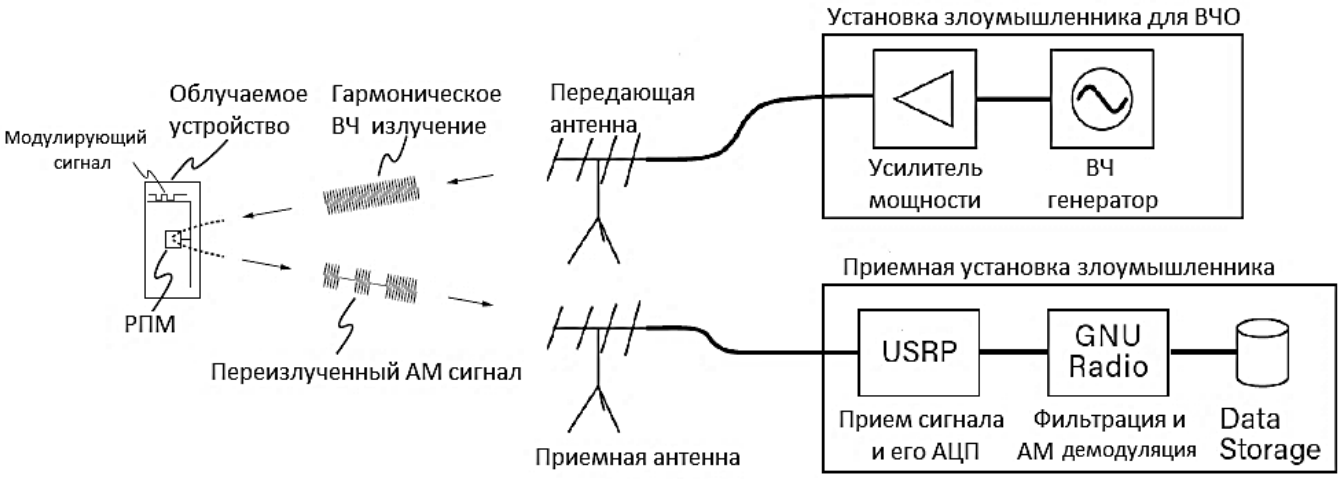

Рис. 12. Функциональная схема для реализации активной атаки с использованием РОМ.

нала позволяет обеспечить помехоустойчивость передаваемых данных. Для организации активной атаки на USB-клавиатуру достаточно установки РОМ в одну из двух сигнальных линий, D+ или D–. В [10] рассматривается установка РОМ на линию D+ (рис. 7), а в [6] — на линию D– (рис. 8).

В USB интерфейсе определяющая роль отведена хосту, который начинает все транзакции. Хост периодически отправляет запрос «IN», опрашивая клавиатуру для «поддержания активности» и не давая ей уходить в «спящий» режим. Если на клавиатуре нажата какая-либо клавиша, клавиатура вернет эту информацию на хост компьютера.

На рисунке 9 показан процесс ввода информации о нажатой на клавиатуре клавише «A» и схема передаваемых сигналов связи.

Первый пакет (Token packet) содержит информацию (рис. 10) об устройстве USB, подключенном к персональному компьютеру. Следующий пакет (Data packet) несет полезную нагрузку, за которым идет завершающий пакет (Handshake packet), сообщающий о том, что данные были приняты успешно, или конечная точка (endpoint) остановлена (stalled) или недоступна для принятия данных.

Двоичный код сканирования, содержащий информацию о нажатой клавише, занимает определенные позиции в пакете данных (рис. 11). [2]

После приема и АМ-демодуляции переотраженного сигнала от РОМ злоумышленник восстанавливает двоичную последовательность, обнаруживает преамбулу и декодирует двоичные данные с целью восстановления комбинации, соответствующей нажатой клавише.

3. Сбор информации

Реализация активных атак на VGA-монитор и USB-клавиатуру может быть реализована (при условии заранее

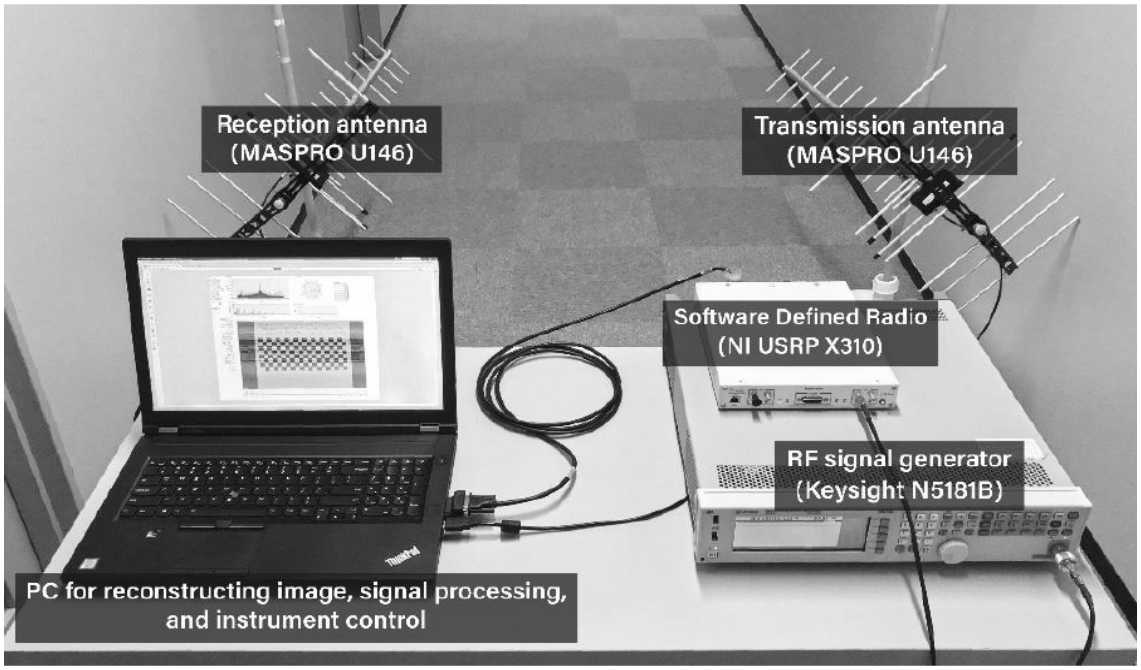

Рис. 13. Внешний вид оборудования для реализации активной атаки

встроенного РОМ) при помощи установки, функциональная схема которой представлена на рис. 12.

Атакующая часть установки злоумышленника состоит из генератора высокочастотных сигналов, усилителя мощности и передающей антенны. Генератор сигналов позволяет генерировать синусоидальное колебание необходимой частоты, совпадающее с резонансной частотой непреднамеренной антенны, на которую нагружен РОМ. Для успешной атаки значение частоты облучения может быть подстроено под одно из резонансных значений для непреднамеренной антенны облучаемого ТС. Генерируемый синусоидальный сигнал усиливается усилителем мощности с возможностью регулировки величины выходного сигнала и транслируется в передающую антенну. Направленная передающая антенна ориентирована таким образом, чтобы облучаемое ТС находилось в максимуме диаграммы направленности.

В соответствие с описанным ранее механизмом утечки информации с использованием РОМ непреднамеренная антенна облучаемого ТС излучает АМ сигнал, модулированный целевым информационным сигналом утечки.

Приемная часть установки злоумышленника содержит приемную антенну, настраиваемую радиоплатформу SDR (Software-defined radio), выдающую уже демодулированный сигнал, и ПК, обеспечивающий его дальнейшую обработку.

В [9] рассматривается установка злоумышленника для проведения активных атак (рис. 13) на базе следующего оборудования:

- приемная и передающая антенны — MASPRO U146 (коэффициент усиления 8~12.4 dB);
- генератор ВЧ сигналов Keysight N5181B (диапазон частот 9 кГц — 6 ГГц, выходная мощность на частоте 1 ГГц –144…+26 дБм);
- усилитель мощности R&K A000110–4040-R (диапазон частот 1–1000 МГц, коэффициент усиления +40 dB);
- SDR радиосплатформы Ettus USRP X310 (диапазон частот сигналов от постоянного тока до 6 ГГц, частота оцифровки АЦП — 200 МВыб/с, разрешение АЦП — 14 бит);
- программное обеспечение SDR радиоплатформы — GNU Radio 3.7.12.

Реализуемость активной атаки на ТС, в которые внедрен РОМ, определяется следующими факторами:

- частота гармонического сигнала, используемого для ВЧО технического средства, соответствует резонансной частоте составной коммуникационной линии, состоящей из интерфейсного кабеля и проводников на печатной плате, которая выступает как непреднамеренная антенна;
- мощность сигнала ВЧО позволяет формировать уровень переотраженного сигнала, достаточный для его приема с уровнем ошибок, не превышающим заданный порог;

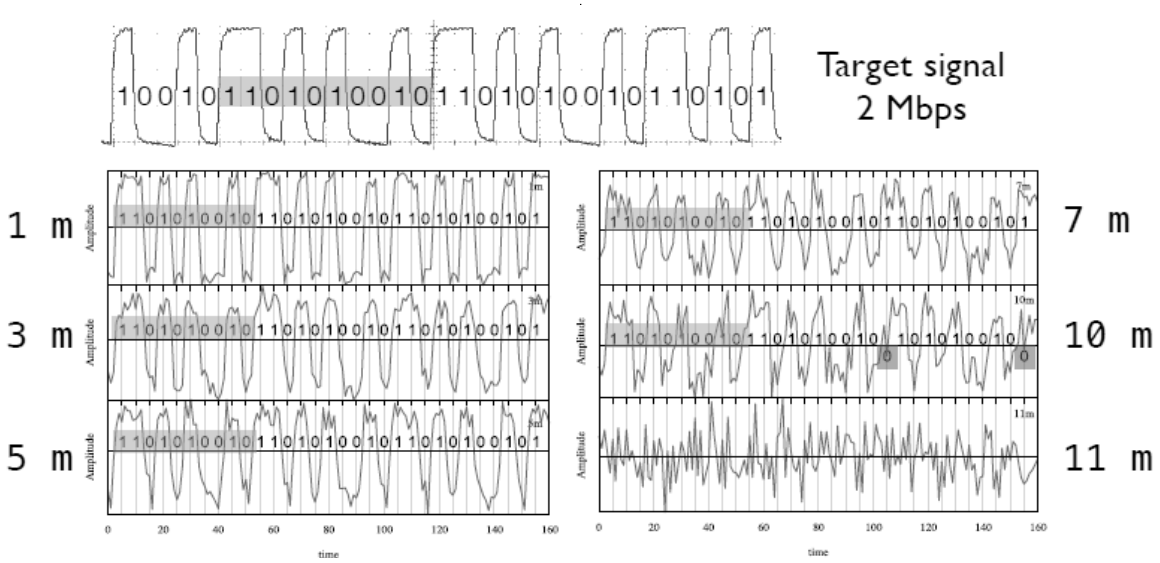

Рис. 14. Зависимость формы переотраженного сигнала от расстояния до атакуемого ТС

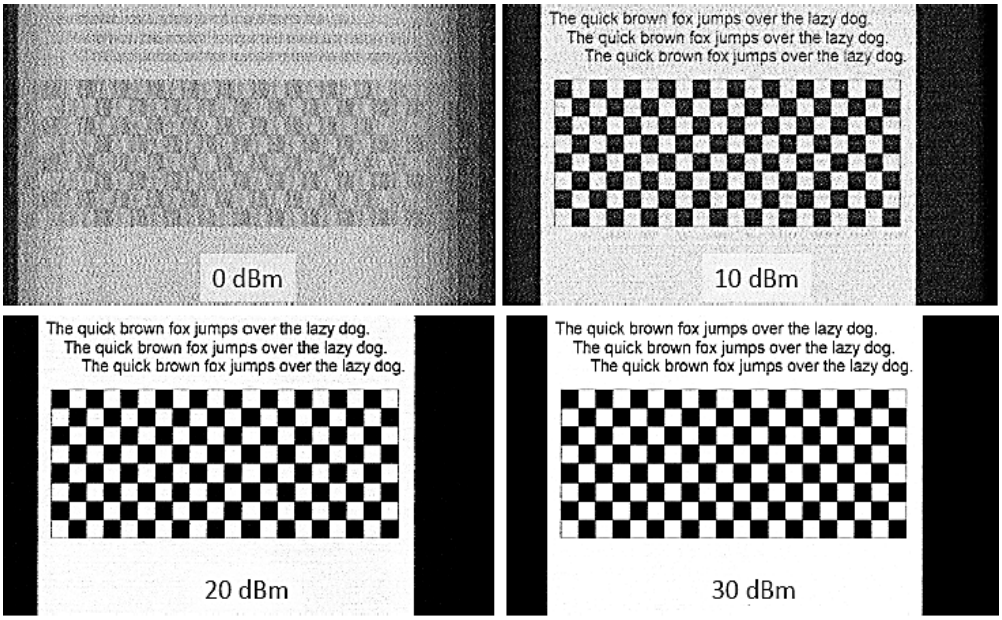

Рис. 15. Зависимость качества сигнала от мощности ВЧО

- частота модулирующего сигнала данных не превышает рабочей частоты активного элемента, на котором выполнен РОМ;
- быстродействие АЦП, применяемой SDR радиоплатформы, позволяет реализовать прямую или полосовую дискретизацию переизлученного сигнала.

Быстродействие АЦП современных SDR радиоплатформ составляет несколько сотен Мвыб/с при разрядности до 12–14 бит, что позволяет при обработке сигналов с частотами, не превышающими несколько десятков МГц, использовать классический принцип дискретизации в соответствии с теоремой Котельникова. При этом оцифровке подвергается диапазон частот от постоянной составляющей до половины частоты дискретизации, и на входе АЦП достаточно использовать ФНЧ для защиты от наложения спектров.

Для высокочастотных сигналов используется полосовая дискретизация (under sampling), которая позволяет обойти ограничение, накладываемое теоремой Котель-

никова (частота выборок должна быть как минимум в два раза больше верхней частоты в спектре дискретизируемого сигнала) для обработки узкополосных сигналов, у которых ширина спектра много меньше абсолютного значения центральной частоты. Этому условию соответствуют практически все радиосигналы. В этом случае теорема Котельникова звучит следующим образом: для сохранения информации о сигнале частота его дискретизации должна быть равной или большей, чем удвоенная ширина его полосы. Математически условие, которое должна выполнять частота дискретизации, описывается выражением:

$$(2fc-B)/m \geq fs \geq (2fc+B)/m+1$$

где: f_C — центральная частота в спектре сигнала; fs — частота дискретизации; B — ширина спектра сигнала; m — произвольное целое число, выбираемое таким образом, чтобы выполнялось соотношение $f_S \geq 2B$.

При полосовой дискретизации оцифровке подвергается не вся полоса частот, а лишь небольшая ее часть. При этом для защиты от наложения спектра необходимо использовать полосовые аналоговые фильтры. Стоит также отметить, что полосовая дискретизация позволяет одновременно с оцифровкой сигнала произвести перенос его спектра на низкую частоту.

В обоих случаях на входе преобразователя необходимо использовать аналоговые фильтры для защиты от наложения спектра. При этом, чем выше частота дискретизации, тем менее жесткие требования предъявляются к аналоговому фильтру. На практике разработчики стараются обеспечить такую частоту дискретизации, чтобы на входе АЦП было достаточно использовать трех- или четырехкаскадный пассивный фильтр.

В [6, 10] рассматривается реализация объекта атаки по схеме, представленной на рис. 12. Мощность сигнала ВЧО составляла 10 dBm, а частота варьировалась в диапазоне 590–680 МГц, что примерно соответствует резонансной частоте непреднамеренной антенны. РОМ модулировался повторяющейся 10-битовой комбинацией «1101010010». Напряжение сигнала составляло 3 V, а скорость передачи — 2 Мбит/с. Частота дискретизации была выбрана 10 МВыб/с.

На рисунке 14 представлены формы сигналов для расстояний атаки, составляющей 1 м, 3 м, 5 м, 7 м, 10 м и 11 м.

Активная атака на ТС при указанных условиях может быть осуществлена с расстояния менее 10 метров из-за возникающих ошибок при приеме переотраженного сигнала, что приводит к искажению модулирующей комбинации.

Зависимость качества восстановленного сигнала от мощности ВЧО иллюстрируется рис. 15. [9]

Заключение

Анализируя данные, полученные в [2, 5, 6, 9, 10], можно утверждать о реализуемости активной атаки на ТС, в которые внедрен РОМ, при соблюдении определенных ограничений для дистанции атаки. Полученная дальность атаки в 10 м и возможность восстановления перехватываемого сигнала, транслируемого/обрабатываемого в ТС со скоростями до 2 Мбит/с не является предельными.

Дальность атаки может быть повышена при условии использования для приема и первичной обработки переотраженного сигнала SDR радиоплатформы с быстродействующим АЦП (например, АЦП платформы USRP Ettus X310 обеспечивает 200 Мвыб/с при разрядности 14 бит), а также при увеличении мощности сигнала ВЧО. При этом необходимо будет учитывать, что с увеличении мощности сигнала ВЧО будет возрастать и демаскирующий фактор процесса облучения.

Учитывая миниатюрность элементной базы, применяемой при изготовлении РОМ; возможность встраивания ЭУНПИ на этапе изготовления или модернизации ТС, данная активная атака позволяет реализовать на практике канал утечки конфиденциальной информации.

ЛИТЕРАТУРА

1. Hayashi Y., Homma N., Miura M., Aoki T., And Sone, H. A threat for tablet pcs in public space: Remote visualization of screen images using EM emanation. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (2014), CCS '14, ACM, pp. 954–965.
2. Kinugawa M., Fujimoto D., & Hayash, Y. Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(4), 62–90.
3. Паршаков В.Р., Лобашев А.К. Проблемы и особенности обнаружения закладочных устройств — эндовибраторов. Информационно-методический журнал «Защита Информации. Инсайд» № 2 (62).
4. Хореев А.А. Техническая защита информации. Том 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008.
5. Wakabayashi S. Investigation of Radio Frequency Retroreflector Attacks. http://hdl.handle.net/2065/00061830

6. Wakabayashi S., Maruyama S., Mori T., Goto S., Kinugawa M., Hayashi Y.-I. POSTER: Is active electromagnetic side-channel attack practical. 24th ACM SIGSAC Conference on Computer and Communications Security, CCS2017; Dallas; United States; 30 October- 3 November 2017.
7. H.S. Lee, D.H. Choi, K. Sim and J. Yook, "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Environment," in IEEE Transactions on Electromagnetic Compatibility, vol. 61, no. 4, pp. 1098–1106, Aug. 2019.
8. P. De Meulemeester, L. Bontemps, B. Scheers and G.A.E. Vandenbosch, "Synchronization retrieval and image reconstruction of a video display unit exploiting its compromising emanations," 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, 2018, pp. 1–7.
9. Kinugawa M., Fujimoto D., & Hayashi Y. Electromagnetic Information Extortion from Electronic Devices Using Interceptor, Its Countermeasure. https://tches.iacr.org/index.php/TCHES/article/view/8345/7839.
10. Wakabayashi S., Maruyama S., Mori T., Goto S., Kinugawa M., Hayashi Y.-I. A Feasibility Study of Radio-frequency Retroreflector Attack. WOOT'18: Proceedings of the 12th USENIX Conference on Offensive Technologies, August 2018.

Московский государственный технический университет имени Н.Э. Баумана