Сергей В. Скрыль[1], Екатерина В. Вайц[2], Сергей С. Никулин[3],
Роман А. Цой[4], Варвара А. Антонова[5]
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет),
ул. 2-я Бауманская, 5, Москва, 105005, Россия
[1]*e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255*
[2]*e-mail: vaitcev@yandex.ru, https://orcid.org/0000-0002-4629-6252*
[3]*e-mail: nikcc@mail.ru, https://orcid.org/0000-0002-4723-7844*
[4]*e-mail: romabmstu@bmstu.ru, https://orcid.org/0000-0002-2454-3224*
[5]*e-mail: varvara_zi@mail.ru, https://orcid.org/0000-0002-6467-5002*

ТЕХНОЛОГИЯ SOFT TEMPEST КАК ОБЪЕКТ ФУНКЦИОНАЛЬНОГО МОДЕЛИРОВАНИЯ

DOI: http://dx.doi.org/10.26583/bit.2022.1.11

Аннотация. Данная статья посвящена представлению технологии программно-управляемого побочного электромагнитного излучения (технологии Soft Tempest (ST)) и процессов противодействия утечке информации по ST-каналу в терминах функционального моделирования. Подобное представление является средством первичной формализации действий нарушителя по внедрению вредоносного программного обеспечения (ВПО) в рабочую среду СВТ для инициализации побочных электромагнитных излучений (ПЭМИ) от электронного оборудования СВТ, а также противодействию утечке информации по каналу рассматриваемого типа. Представлен общий механизм декомпозиции целевых функций «Перехват нарушителем информативных сигналов СВТ по ST-каналу» и «Противодействие утечке информации по ST-каналу». Обосновываются классификационные основания для трехуровневой детализации данных целевых функций. Приводятся результаты детализации действий нарушителя на отдельные этапы, реализуемые мероприятия по противодействию утечке информации, выполняемые нарушителем процедуры, принимаемые меры противодействия и соответствующие этим процедурам и мерам функции. Полученные результаты являются предпосылкой для формализованного представления описываемых процессов в терминах Марковских процессов и разработки математических моделей, соответствующих временных и вероятностных характеристик для количественной оценки возможностей нарушителя по реализации угроз перехвата побочных электромагнитных излучений от электронного оборудования СВТ, вызванных воздействием ВПО.
Ключевые слова: технология Soft Tempest, ST-канал утечки информации, перехват информативных сигналов, противодействие утечке информации по ST-каналу, программно-управляемое побочное электромагнитное излучение.
Для цитирования: СКРЫЛЬ, Сергей В. и др. ТЕХНОЛОГИЯ SOFT TEMPEST КАК ОБЪЕКТ ФУНКЦИОНАЛЬНОГО МОДЕЛИРОВАНИЯ. Безопасность информационных технологий, [S.l.], т. 29, № 1, p. 125–144, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1412. DOI: http://dx.doi.org/10.26583/bit.2022.1.11.

Sergey V. Skryl[1], Ekaterina V. Vaitc[2], Sergey S. Nikulin[3], Roman A. Tsoy[4],
Varvara A. Antonova[5]
Bauman Moscow State Technical University (National Research University),
2nd Bauman Str., 5, Moscow, 105005, Russia
[1]*e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255*
[2]*e-mail: vaitcev@yandex.ru, https://orcid.org/0000-0002-4629-6252*
[3]*e-mail: nikcc@mail.ru, https://orcid.org/0000-0002-4723-7844*
[4]*e-mail: romabmstu@bmstu.ru, https://orcid.org/0000-0002-2454-3224*
[5]*e-mail: varvara_zi@mail.ru, https://orcid.org/0000-0002-6467-5002*

Soft tempest technology as an object of functional modeling

DOI: http://dx.doi.org/10.26583/bit.2022.1.11

Abstract. This article focuses on presenting the software-controlled transient electromagnetic pulse emanation technology (Soft Tempest (ST) technology) and the ST-channel information leakage counteraction in terms of functional modeling. Such a representation is a means of primary formalization of the actions of the intruder to prepare the implementation malicious software into the CT working environment to initiate a transient electromagnetic pulse emanation (TEMPE) from electronic equipment of CT and also formalization of countering of information leakage via reviewed channel. The general mechanism of decomposition of the target functions «Intruder interception of informative signals of CE via ST-channel» and «Counteracting information leakage via the ST-channel» is presented in this article. The classification basis for the three-level detailing of these target functions is substantiated. The report provides the results of detailing the actions of the intruder into certain stages, the ongoing activities to counteract information leakage, the processes taken by the intruder, taken countermeasures and the functions corresponding to these processes and countermeasures. The results thus obtained are a prerequisite for the formalized representation of the processes described in terms of Markov processes and the development of mathematical models of the related temporal and stochastic characteristics to quantitatively measure the ability of the intruder to realize the threats of interception of a TEMPE from the electronic equipment of CT, caused by malware.

Keywords: Soft Tempest technology, information leakage, interception of informative signals of computers technique (CT) via the ST-channel, software-controlled transient electromagnetic pulse emanation.

For citation: SKRYL, Sergey V. et al. Soft tempest technology as an object of functional modeling. IT Security (Russia), [S.l.], v. 29, n. 1, p. 125–144, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1412. DOI: http://dx.doi.org/10.26583/bit.2022.1.11.

Введение

Анализ ретроспектив технической разведки (ТР), как способа перехвата информативных сигналов физических полей, содержащих конфиденциальную информацию; и перспектив дальнейшего совершенствования ТР позволяет выявить устойчивую тенденцию к целенаправленному совершенствованию способов и средств перехвата компьютерной информации по каналам побочных электромагнитных излучений (ПЭМИ) [1–4]. Это обусловлено, главным образом совершенствованием технологии электронного документооборота, в результате которого огромное количество конфиденциальной информации аккумулируется в электронных документах. В отличие от традиционного способа несанкционированного получения конфиденциальной информации техническими средствами разведки – путем перехвата отдельных речевых сообщений, перехват электронного документа, позволяет обеспечить высокую степень целостности перехваченной информации. Вместе с тем, существуют и специфичные технические каналы утечки информации, комбинирующие программные способы воздействия на информационную среду и способы перехвата информативных сигналов физических полей [5]. Подобная технология перехвата компьютерной информации получила широкую известность как технология скрытой передачи данных по каналу ПЭМИ с помощью программных средств – Soft Tempest (ST) [5]. В отечественной литературе по технической защите информации подобный способ перехвата компьютерной информации получил название программно-управляемое побочное электромагнитное излучение. ST-технология, по своей сути, есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в видео, аудио, графических и текстовых файлах [6].

Высокая скрытность такого рода канала утечки информации обусловила необходимость его исследования с целью научного обоснования требований к характеристикам применяемых способов и средств противодействия данному, весьма специфичному, виду технической разведки.

Следует отметить, что существующая практика обоснования подобного рода требований, вследствие своей эмпирической природы, не обеспечивает обоснованность этих решений.

Очевидно, что обоснованность решений относительно направлений совершенствования механизмов защиты информации от утечки по ST-каналу должна основываться на адекватной оценке возможностей противодействия утечке.

Следует отметить, что применение с этой целью существующего методического аппарата оценки характеристик безопасности информационных технологий, связано с рядом проблем. Наиболее значимыми из них являются:

1) отсутствие формальных оснований для представления угрозы утечки информации по ST-каналу как действий нарушителя по ее реализации, и как следствие, ограниченное число состояний, характеризующих такого рода угрозу;

2) необходимость оценки комплексного влияния на процесс противодействия утечке информации по ST-каналу двух, существенно различных по своей природе, механизмов предотвращения такого рода угрозы – антивирусного и технического контроля.

3) отсутствие математической интерпретации ряда случайных событий, характеризующих динамику угрозы утечки информации по ST-каналу и его обнаружения средствами защиты от такого рода угроз.

Это не позволяет использовать существующий методический аппарат оценки характеристик безопасности информационных технологий для адекватной оценки возможностей по реализации угроз утечки информации по ST-каналу и, как следствие, в качестве инструмента формирования обоснованных решений относительно характеристик применяемых способов и средств противодействия.

Целью данной статьи является обоснование возможностей преодоления обстоятельств, обусловленных первыми двумя, из перечисленных выше проблем за счет применения методологии функционального моделирования, позволяющей определить все возможные состояния как процесса реализации угроз утечки информации по ST-каналу, так и процесса противодействия данному виду технической разведки.

1. Особенности формирования ST-канала утечки информации

Исследования по разработке тестовых сигналов для анализа интерфейсов средств вычислительной техники (СВТ), выполненные Маркусом Куном (Markus G. Kuhn) в 1998 г. в лаборатории Кембриджского университета, продемонстрировали возможность формирования нового типа технического канала утечки информации. Суть исследований состояла в том, что объект воздействия (СВТ) «заражается» вредоносной программой со специализированными возможностями. Такого рода программа ищет необходимую информацию в памяти СВТ и путем обращения к различным его устройствам вызывает появление ПЭМИ. Например, вредоносная программа может встраивать сообщение в сигнал монитора, при этом пользователь не подозревает, что в изображение на экране монитора вставлены определенные текстовые сообщения или изображения. С помощью разведывательного приемника обеспечивается перехват паразитного излучения монитора и выделение требуемого полезного сигнала.

Высокая эффективность ST-технологии, как разновидности угроз безопасности компьютерной информации, достигается за счет скрытности работы вредоносной программы.

В отличие от традиционного способа использования вредоносных программ в качестве источника угроз нарушения конфиденциальности информации в компьютерной сети [7], применение ST-технологии не предполагает рассылку несанкционированного

скопированных данных по сети, что позволяет в течение длительного времени не обнаруживать утечку информации соответствующими антивирусными средствами. Поэтому, вредоносные программы, использующие в качестве физической среды для передачи данных ПЭМИ электронного оборудования СВТ, могут работать годами, не обнаруживая себя.

В случае автономной работы СВТ ST-технология является для нарушителя единственным способом получения конфиденциальной информации, обрабатываемой данным средством.

В 2001 г. Эрик Тиле (Erik Thiele), основываясь на работе Маркуса Куна [8] представил программу Tempest for Eliza, позволяющую использовать VGA интерфейс в качестве генератора радиосигнала с амплитудной модуляцией.

Качественное развитие технология передачи данных за счёт ПЭМИ получила в 2014 г., когда Мордехай Гури (Mordechai Guri) с коллегами представили работу AirHopper [9]. В работе реализована возможность передачи информации по каналу ПЭМИ, с возможностью приема информации на встроенный приемник мобильного телефона или смартфона.

Уильям Энтрикен (William Entriken) воодушевившись работами Гури опубликовал программное обеспечение (ПО), позволяющее осуществлять амплитудную модуляцию (АМ) излучения шины памяти (I/O bus clock) при обмене данными между CPU и RAM.

Авторы исследования смогли добиться скорости передачи порядка 1000 бит/с на расстоянии 2,6 м, при использовании SDR-приемника.

В августе 2015 г. Гури представил программное обеспечение GSMem, формирующее радиоканал передачи данных на частотах сетей сотовой связи GSM, UMTS и LTE, а также в диапазоне частот Wi-Fi. Данное ПО использует специфические инструкции процессора, непрерывно изменяя несущие частоты многоканальной памяти. Авторам удалось добиться стабильной скорости передачи 1000 бит/с на расстоянии в 2 м, прием осуществлялся на мобильные телефоны.

В 2016 г. Мордехай Гури представил способ передачи информации за счёт ПЭМИ USB-интерфейса, добившись скорости 80 байт/с в процессе манипуляции несущей частоты интерфейса при передаче данных по нему. В качестве антенны выступал сам интерфейс и подключенный к нему флеш-накопитель. Метод передачи получил название USBee [10].

Стоит отметить, что исследования Гури не ограничились формированием радиоканалов, так на данный момент представлены способы передачи информации от изолированного от внешних подключений СВТ с помощью:

– световых волн мерцания светодиода во время работы жесткого диска 20 бит/с при использовании обычной видеокамеры для фиксации;

– звуковых волн, формируемых шумом вентилятора 900 байт/ч;

– периодически появляющихся кадров низкой контрастности от современных LCD мониторов, которые могут быть восстановлены при помощи камеры;

– термальных флуктуаций СВТ (с помощью ПО BitWhisper до 10 бит/час на расстоянии полуметра) [11].

Таким образом, наличие в составе СВТ аппаратных составляющих, способных излучать ПЭМИ и возможность программного управления режимами работы СВТ, обеспечивают модуляцию этих излучений информационными сигналами. В результате формируется ST-канал утечки информации.

В табл.1 приводится характеристика известных способов реализации ST-технологии.

Таблица 1. Сравнение известных способов передачи информации посредством модуляции ПЭМИ от СВТ

Наименование способа передачи	**Источник излучения**	**Достигнутая скорость**	**Порядок дальности приема**
Markus G. Kuhn Soft Tempest, 1999 г	Электронно-лучевая трубка	-	1 км
AirHopper, 2014 г.	Интерфейс VGA	8 байт/с	100 м
GSMem, 2015 г.	Системная шина данных (front-side)	1000 бит/с	20 м
USBee, 2016 г.	USB интерфейс	80 байт/с	30 м

Возможность модуляции ПЭМИ информацией, обрабатываемой СВТ, но непосредственно не передающейся в излучающем интерфейсе в нормальном режиме работы, является ключевой особенностью и главным отличием ST-технологии от классического перехвата информационных сигналов ПЭМИ. Их сравнение представлено в табл. 2.

Таблица 2. Сравнение классического перехвата информационных сигналов ПЭМИ и ST-технологии

	Классический перехват информационных сигналов ПЭМИ	**ST-технология**
Носитель информации	ПЭМИ	ПЭМИ
Источник сигнала	Интерфейс, участвующий в обработке информации	Любой интерфейс, излучающий ПЭМИ и допускающий программное управление
Передаваемая (излучаемая) информация	Информация, обрабатываемая излучающим интерфейсом	Любая информация ограниченного доступа, к которой имеет доступ программа, формирующая ПЭМИ
Скорость передачи информации	Определяется длительностью импульса тактовой частоты излучающего интерфейса	Определяется временем изменения параметров интерфейса
Тип передаваемого сигнала	Широкополосный	Узкополосный
Условия формирования технического канала утечки информации	Зона, в которой возможен перехват ПЭМИ с помощью разведывательного приемника, с последующей расшифровкой, содержащейся в них информации, больше расстояния до границы контролируемой зоны	Программная закладка в СВТ

Результаты экспериментальных исследований по формированию канала передачи данных, основанного на ST-технологии некоторых интерфейсов СВТ представлены в табл. 3.

Таблица 3. Сравнение каналов передачи информации основанных на ST-технологии интерфейсов СВТ

Излучающий ST-интерфейс	**Модуляция**	**Экспериментально достигнутая дальность приема без когерентного накопления**	**Экспериментально достигнутая скорость передачи информации**
VGA	ФМ, ЧМ	80 м	400 бит/с
DVI, HDMI	АМ	6 м	20 бит/с
PCI, PCI-E	ЧМ	10 м	100 бит/с
FSB	ЧМ	7 м	100 бит/с
GPU	АМ	1 м	1 бит/с

Таким образом, очевидно, что ST-технология, как объект противодействия техническим разведкам, нуждается в глубоком изучении.

2. Формализованное представление действий нарушителя по перехвату информативных сигналов СВТ по ST-каналу

Обоснование требований к способам и средствам противодействия утечке информации по ST-каналу предполагает наличие соответствующего методического аппарата, позволяющего адекватно оценить как характеристики такого рода канала, так и характеристики средств противодействия утечке. Рассмотрим возможность применения для решения данной проблемы классической методологии исследования – теории моделирования.

К настоящему времени в методологии моделирования в целом и в теории и практике противодействия техническим разведкам, в частности, сформирована довольно обширная методическая база функционального моделирования исследуемых процессов, как средства их первичной формализации [12]. При этом выделяются две наиболее распространенные формы представления этих моделей: представление в виде функциональных диаграмм [13] и представление в виде графов [14]. Обе формы представления позволяют отразить все детали функциональных компонент исследуемых процессов в рамках иерархии их функциональной декомпозиции.

Функциональные диаграммы представляют собой довольно наглядное средство интерпретации всех деталей информационных процессов со сложной функциональной структурой: внутренний интерфейс функциональных компонент, интерфейс с внешней информационной средой, условия реализации исследуемых информационных процессов и используемые при этом ресурсы. Вместе с тем опыт применения методического аппарата для функционального моделирования информационных процессов, представляемых как отдельные состояния, реализуемые в однотипной информационной среде с ограниченной номенклатурой средств, позволяет утверждать о существенной избыточности функциональных диаграмм как инструмента первичной формализации.

Этого недостатка лишено представление этих процессов в виде декомпозиционной структуры графов. Подобное функциональное описание содержит лишь необходимые для идентификации функций параметры: перечень реализуемых состояний, характеристики нахождения процессов в этих состояниях и порядок смены состояний. Все эти параметры на каждом из уровней функциональной декомпозиции исследуемого процесса представляются в виде графа. Как и в случае функционального описания с помощью функциональных диаграмм представление исследуемых процессов в виде декомпозиционной структуры графов дает возможность отразить функциональную иерархию этих процессов, получаемую в результате декомпозиции реализуемых функций.

Проиллюстрируем эти возможности для формализации ST-технологии.

В основе такой иерархии лежит представление целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» в наиболее обобщенном виде – в виде одного состояния, реализующего данную целевую функцию. Подобное представление в терминах декомпозиционной структуры графов определяется как концептуальная функциональная модель процессов, связанных реализацией такого рода угрозы безопасности информации (функциональная модель нулевого уровня).

Детализация концептуальной функциональной модели этих процессов позволяет выявить набор подфункций, реализующих вышеуказанную целевую функцию. Этот набор образует первый уровень декомпозиционной структуры графов, описывающих процессы реализации ST-технологии.

Выявление набора подфункций для любой функции исследуемых процессов позволяет формировать следующие уровни их функциональной иерархии.

Декомпозиция может быть завершена в том случае, когда набор подфункций может быть описан терминами цепей Маркова [15].

При формировании функциональной модели процессов перехвата нарушителем информативных сигналов СВТ по ST-каналу воспользуемся результатами анализа практики реализации такого рода угроз безопасности информации.

Первый уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» составляют подфункции подготовки к реализации такого рода угрозы, внедрения вредоносного кода, его распространение в рабочей среде СВТ, обнаружение и перехват информативных сигналов ПЭМИ от электронного оборудования СВТ, а также обработки перехваченной информации [16]. Данные подфункции следует рассматривать как этапы реализации целевой функции (рис. 1):

$Э_1$ – этап подготовки к перехвату информативных сигналов СВТ по ST-каналу;

$Э_2$ – этап внедрения вредоносного кода в рабочую среду СВТ;

$Э_3$ – этап инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ;

$Э_4$ – этап обнаружения ПЭМИ от электронного оборудования СВТ;

$Э_5$ – этап перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ;

$Э_6$ – этап обработки информативных сигналов от электронного оборудования СВТ.

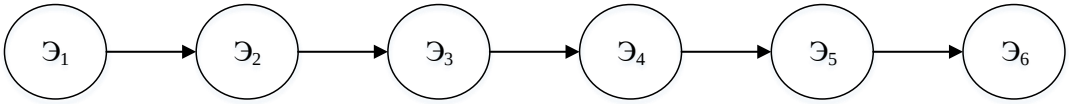

Рис. 1. Декомпозиционное представление целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу»
Fig. 1. Decomposition view of the target function «Intruder interception of informative signals of CT via ST-channel»

Второй уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» образуется путем детализации действий нарушителя, выполняемых им в процессе реализации этапов $Э_1$–$Э_6$. Соответствующие данному уровню действия следует рассматривать как процедуры реализации указанных этапов.

К процедурам, реализующим этап $Э_1$ подготовки к перехвату информативных сигналов СВТ по ST-каналу, относятся (рис. 2):

$П_{11}$ – процедура сбора информации об объекте угрозы утечки информации по ST-каналу;

$П_{12}$ – процедура разработки соответствующего вредоносного кода.

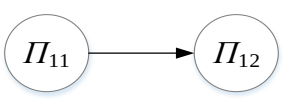

Рис. 2. Декомпозиционное представление этапа подготовки к перехвату информативных сигналов СВТ по ST-каналу
Fig. 2. Decomposition view of the stage of preparation for the interception of informative signals of computer equipment via ST-channel

К процедурам, реализующим этап $Э_2$ внедрения вредоносного кода в рабочую среду СВТ, относятся (рис. 3):

$П_{21}$ – процедура получения доступа к рабочей среде СВТ;

$П_{22}$ – процедура внедрения вредоносного кода в рабочую среду СВТ;

$П_{23}$ – процедура сокрытия работы вредоносного кода.

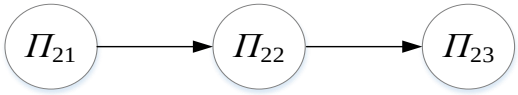

Рис. 3. Декомпозиционное представление этапа внедрения вредоносного кода в рабочую среду СВТ

Fig. 3. Decomposition view of the stage of the malware implementation in the working environment of CT

К процедурам, реализующим этап $Э_3$ инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ, относятся (рис. 4):

$П_{31}$ – процедура определения вредоносным кодом доступных интерфейсов передачи данных в рабочей среде СВТ;

$П_{32}$ – процедура обнаружения информации, являющейся целью перехвата;

$П_{33}$ – процедура кодирования информации, являющейся целью перехвата;

$П_{34}$ – процедура формирования программного инструментария для реализации воздействия на интерфейс передачи данных в рабочей среде СВТ;

$П_{35}$ – процедура реализации воздействия на интерфейс передачи данных в рабочей среде СВТ.

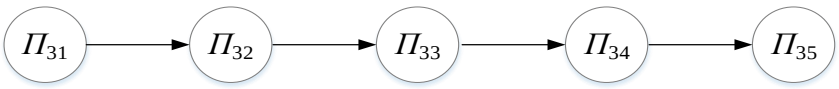

Рис. 4. Декомпозиционное представление этапа инициализации вредоносным кодом ПЭМИ от электронного оборудования СВТ

Fig. 4. Decomposition view of the stage the malware initiation of a transient electromagnetic pulse emanation (TEMPE) from electronic equipment of CT

К процедурам, реализующим этап $Э_4$ обнаружения ПЭМИ от электронного оборудования СВТ, относятся (рис. 5):

$П_{41}$ – процедура определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{42}$ – процедура верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ.

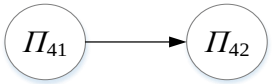

Рис. 5. Декомпозиционное представление этапа обнаружения ПЭМИ от электронного оборудования СВТ

Fig. 5. Decomposition view of the stage of detection of the TEMPE from electronic equipment of CT

К процедурам, реализующим этап $Э_5$ перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ, относятся (рис. 6):

$П_{51}$ – процедура настройки технического средства разведки (ТСР) для приема информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{52}$ – процедура приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ.

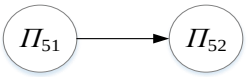

Рис. 6. Декомпозиционное представление этапа перехвата информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 6. Decomposition view of the stage interception of informative signals of the TEMPE from electronic equipment of CT

К процедурам, реализующим этап $Э_6$ обработки информативных сигналов от электронного оборудования СВТ, относятся (рис. 7):

$П_{61}$ – процедура демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ;

$П_{62}$ – процедура обработки перехваченной информации с целью обеспечения ее целостности.

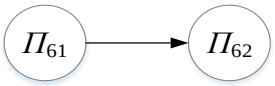

Рис. 7. Декомпозиционное представление этапа обработки информативных сигналов от электронного оборудования СВТ
Fig. 7. Decomposition view of the stage of processing of informative signals of the TEMPE from electronic equipment of CT

Третий уровень декомпозиции целевой функции «Перехват нарушителем информативных сигналов СВТ по ST-каналу» образуется путем детализации действий, выполняемых в процессе реализации процедур $П_{11}$–$П_{62}$. Соответствующие данному уровню действия следует рассматривать как функции, реализующие указанные процедуры.

К функциям, реализующим процедуру сбора информации об объекте угрозы утечки информации по ST-каналу (процедуру $П_{11}$), относятся (рис. 8):

$Ф_{111}$ – функция определения режимов использования СВТ для сбора информации об объекте угрозы;

$Ф_{112}$ – функция сбора информации о сотрудниках, допущенных к СВТ;

$Ф_{113}$ – функция сбора информации о времени работы сотрудников с СВТ;

$Ф_{114}$ – функция сбора информации о средствах защиты информации, установленных на СВТ;

$Ф_{115}$ – функция сбора информации о ПО, установленном на СВТ;

$Ф_{116}$ – функция определения возможностей по внедрению вредоносного кода.

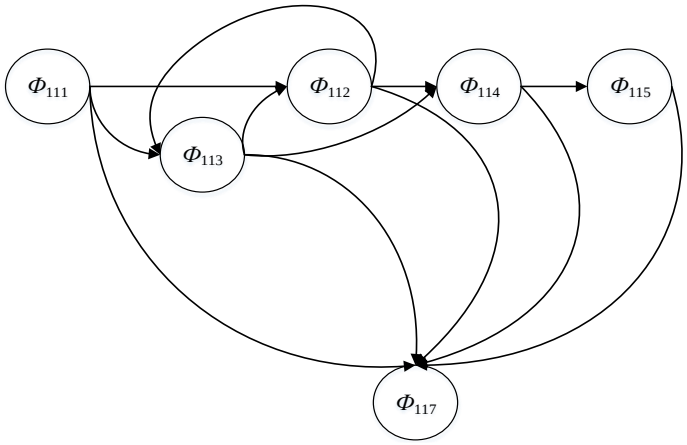

Рис. 8. Декомпозиционное представление процедуры сбора информации об объекте угрозы утечки информации по ST-каналу
Fig. 8. Decomposition view of the procedure for information gathering on the object of information leak threat via ST-channel

К функциям, реализующим процедуру разработки соответствующего вредоносного кода (процедуру $П_{12}$), относятся (рис. 9):

$Ф_{121}$ – функция определения инструментов вредоносного воздействия на электронное оборудование СВТ через его рабочую среду;

$Ф_{122}$ – функция выявления уязвимостей механизмов защиты информации в СВТ;

$Ф_{123}$ – функция использования выявленных уязвимостей.

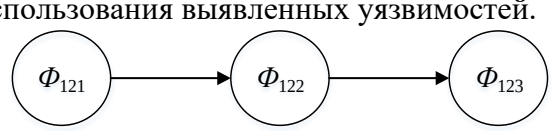

Рис. 9. Декомпозиционное представление процедуры разработки соответствующего вредоносного кода
Fig. 9. Decomposition view of the procedure for developing the appropriate malware

К функциям, реализующим процедуру получения доступа к рабочей среде СВТ (процедуру $П_{21}$), относятся (рис. 10):

$Ф_{211}$ – функция использования доступа, предоставленного третьей стороне;

$Ф_{212}$ – функция использования доверенного носителя информации, содержащего вредоносное ПО;

$Ф_{213}$ – функция несанкционированного подключения внешних устройств.

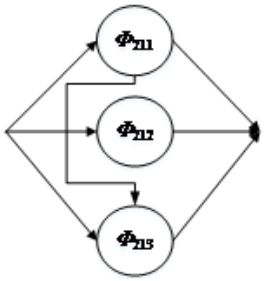

Рис. 10. Декомпозиционное представление процедуры получения доступа к рабочей среде СВТ
Fig. 10. Decomposition view of the procedure for gaining access to the CT workspace

К функциям, реализующим процедуру внедрения вредоносного кода в рабочую среду СВТ (процедуру $П_{22}$), относятся (рис. 11):

$Ф_{221}$ – функция переноса вредоносного кода в рабочую среду СВТ через съемные носители информации;

$Ф_{222}$ – функция переноса вредоносного кода в рабочую среду СВТ через программные компоненты, используя возможности удаленного доступа;

$Ф_{223}$ – функция переноса вредоносного кода в рабочую среду СВТ посредством физического соединения с другими устройствами, входящими в состав СВТ.

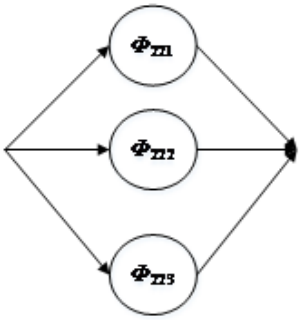

Рис. 11. Декомпозиционное представление процедуры внедрения вредоносного кода в рабочую среду СВТ
Fig. 11. Decomposition view of the procedure for the malware implementation in the working environment of CT

К функциям, реализующим процедуру сокрытия работы вредоносного кода (процедуру $П_{23}$), относятся (рис. 12):

$Ф_{231}$ – функция программного анализа рабочей среды СВТ;

$Ф_{232}$ – функция адаптации вредоносного кода в рабочей среде СВТ.

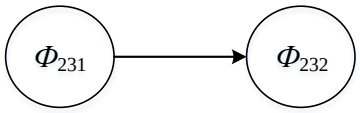

Рис. 12. Декомпозиционное представление процедуры сокрытия работы вредоносного кода
Fig. 12. Decomposition view of the procedure for malware operation concealment

К функциям, реализующим процедуру определения доступных интерфейсов передачи данных в рабочей среде СВТ (процедуру $П_{31}$), относятся (рис. 13):

$Ф_{311}$ – функция проверки наличия доступных интерфейсов передачи данных в рабочей среде СВТ;

$Ф_{312}$ – функция проверки возможности получения доступа к выбранному интерфейсу передачи данных в рабочей среде СВТ.

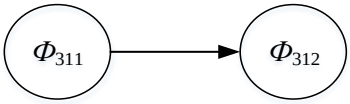

Рис. 13. Декомпозиционное представление процедуры определения доступных интерфейсов передачи данных в рабочей среде СВТ
Fig. 13. Decomposition view of the procedure for identification of available data transmission interfaces in the CT workspace

К функциям, реализующим процедуру обнаружения информации, являющейся целью перехвата (процедуру $П_{32}$), относятся (рис. 14):

$Ф_{321}$ – функция поиска необходимой информации в соответствии с установленными нарушителем параметрами рабочей среды СВТ;

$Ф_{322}$ – функция попытки получения доступа к информации, являющейся целью перехвата, в рабочей среде СВТ.

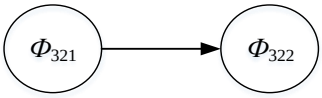

Рис. 14. Декомпозиционное представление процедуры обнаружения информации, являющейся целью перехвата
Fig. 14. Decomposition view of the procedure for detecting information that is the interception target

К функциям, реализующим процедуру кодирования найденной в рабочей среде СВТ информации (процедуру $П_{33}$), относятся (рис. 15):

$Ф_{331}$ – функция подготовки найденной информации к кодированию для выбранного интерфейса передачи данных в рабочей среде СВТ;

$Ф_{332}$ – функция преобразования найденной информации в соответствии с выбранной кодировкой.

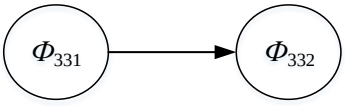

Рис. 15. Декомпозиционное представление процедуры кодирования найденной в рабочей среде СВТ информации
Fig. 15. Decomposition view of the coding procedure for the found information in the CT workspace

К функциям, реализующим процедуру формирования данных для воздействия на интерфейс передачи данных в рабочей среде СВТ (процедуру $П_{34}$), относятся (рис. 16):

$Ф_{341}$ – функция подготовки кодированной информации к формированию пакета данных;

$Ф_{342}$ – функция формирования пакета данных.

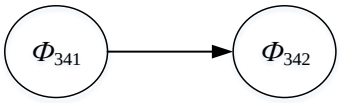

Рис. 16. Декомпозиционное представление процедуры формирования программного инструментария для реализации воздействия на интерфейс передачи данных в рабочей среде СВТ
Fig. 16. Decomposition view of the procedure for forming a software toolkit to influence the data transfer interface in CT work environment

К функциям, реализующим процедуру реализации воздействия на интерфейс передачи данных в рабочей среде СВТ (процедуру $П_{35}$), относятся (рис. 17):

$Ф_{351}$ – функция получения доступа к интерфейсу передачи данных в рабочей среде СВТ;

$Ф_{352}$ – функция циклической отправки пакета данных по интерфейсу передачи данных в рабочей среде СВТ.

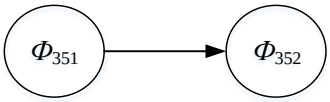

Рис. 17. Декомпозиционное представление процедуры реализации воздействия на интерфейс передачи данных в рабочей среде СВТ
Fig. 17. Decomposition view of the procedure for realization of the impact on the data transfer interface in the CT work environment

К функциям, реализующим процедуру определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{41}$), относятся (рис. 18):

$Ф_{411}$ – функция сканирования спектра электромагнитных сигналов в заданном диапазоне частот;

$Ф_{412}$ – функция обнаружения ПЭМИ в заданном частотном диапазоне;

$Ф_{413}$ – функция определения несущей частоты ПЭМИ.

Рис. 18. Декомпозиционное представление процедуры определения частотного диапазона для обнаружения информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 18. Decomposition view of the procedure for determining the frequency range for detecting informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{42}$), относятся (рис. 19):

$Ф_{421}$ – функция анализа спектра обнаруженного ПЭМИ на несущей частоте;

$Ф_{422}$ – функция верификации обнаруженного ПЭМИ на несущей частоте.

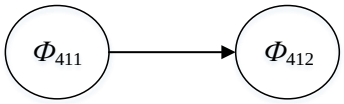

Рис. 19. Декомпозиционное представление процедуры верификации обнаруженных информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 19. Decomposition view of the procedure for verification of detected informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру настройки ТСР для приема информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{51}$), относятся (рис. 20):

$Ф_{511}$ – функция выбора оптимальной измерительной приемной антенны в соответствии с частотным диапазоном;

$Ф_{512}$ – функция выбора оптимального измерительного приемника, в соответствии с заданным частотным диапазоном и полосой пропускания сигнала.

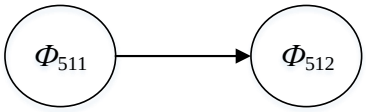

Рис. 20. Декомпозиционное представление процедуры настройки ТСР для приема информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 20. Decomposition view of the procedure for setting up a technical intelligence device (TID) to receive informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{52}$), относятся (рис. 21):

$Ф_{521}$ – функция приема входного электромагнитного сигнала;

$Ф_{522}$ – функция накопления IQ-данных сигналов ПЭМИ;

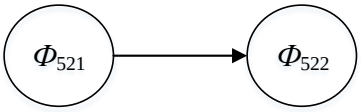

Рис. 21. Декомпозиционное представление процедуры приема и записи информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 21. Decomposition view of the procedure for receiving and recording of informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ (процедуру $П_{61}$), относятся (рис. 22):

$Ф_{611}$ – функция обработки IQ-данных;

$Ф_{612}$ – функция восстановления поврежденных данных.

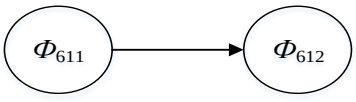

Рис. 22. Декомпозиционное представление процедуры демодуляции перехваченных информативных сигналов ПЭМИ от электронного оборудования СВТ
Fig. 22. Decomposition view of the procedure for the demodulation of intercepted informative TEMPE signals from electronic equipment of CT

К функциям, реализующим процедуру обработки перехваченной информации с целью обеспечения ее целостности (процедуру $П_{62}$), относятся (рис. 23):

$Ф_{621}$ – функция проверки целостности информации;

$Ф_{622}$ – функция ознакомления с информацией.

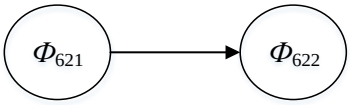

Рис. 23. Декомпозиционное представление процедуры обработки перехваченной информации с целью обеспечения ее целостности
Fig. 23. Decomposition view of the procedure for processing intercepted information in order to ensure its integrity

3. Формализованное представление мер противодействия утечке информации по ST-каналу

Проиллюстрируем возможности функционального моделирования для формализации процессов противодействия утечки информации по ST-каналу.

Основу данной функциональной модели составляет декомпозиционное представление целевой функции «Противодействие утечке информации по ST-каналу». В наиболее обобщенном виде функциональная модель представляется в виде одного состояния, реализующего указанную целевую функцию. Подобное представление в терминах декомпозиционной структуры графов определяется как функциональная модель нулевого уровня.

Детализация функциональной модели целевой функции позволяет выявить набор соответствующих подфункций, которые будут составлять первый уровень декомпозиционной структуры графов, описывающих процессы противодействия утечки информации по ST-каналу.

Выявление набора подфункций для любой функции описывающих исследуемые процессы позволяет формировать следующие уровни их функциональной иерархии.

Процесс функциональной декомпозиции завершается тогда, когда набор подфункций может быть представлен Марковским процессом [15].

Первый уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» составляют подфункции, связанные с изменением программно-аппаратной конфигурации электронного оборудования СВТ, его инструментальной проверкой и техническим контролем эффективности защиты информации от утечки по ST-каналу. Данные подфункции рассматриваются как мероприятия по противодействию утечке информации по ST-каналу (рис. 24):

M_1 – мероприятия по изменению программно-аппаратной конфигурации электронного оборудования СВТ;

M_2 – мероприятия по инструментальной проверке электронного оборудования СВТ;

M_3 – мероприятия по техническому контролю эффективности защиты информации от утечки по ST-каналу.

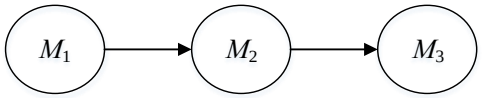

Рис. 24. Декомпозиционное представление целевой функции «Противодействие утечке информации по ST-каналу»
Fig. 24. Decomposition view of the target function «Counteracting information leakage through the ST channel»

Второй уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» образуется путем детализации мероприятий M_1–M_3. Соответствующие данному уровню подфункции рассматриваются как меры, предпринимаемые для реализации указанных мероприятий.

К мерам, предпринимаемым для реализации мероприятий M_1 по изменению программно-аппаратной конфигурации электронного оборудования СВТ, относятся (рис. 25):

E_{11} – меры по изменению конфигурации электронного оборудования СВТ;

E_{12} – меры по замене импортного программно-аппаратного обеспечения СВТ на отечественное.

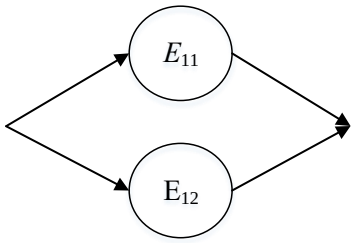

Рис. 25. Декомпозиционное представление мероприятий по изменению программно-аппаратной конфигурации электронного оборудования СВТ
Fig. 25. Decomposition view of the activities for hardware and software configuration changes to electronic equipment of CT

К мерам, предпринимаемым для реализации мероприятий M_2 по инструментальной проверке электронного оборудования СВТ, относятся (рис. 26):

E_{21} – меры по проведению исследований на соответствие требованиям по безопасности информации;

E_{22} – меры по проведению дополнительных исследований.

Рис. 26. Декомпозиционное представление мероприятий по инструментальной проверке электронного оборудования СВТ
Fig. 26. Decomposition view of activities for the instrumental verification of the electronic equipment of CT

К мерам, предпринимаемым для реализации мероприятий M_3 по техническому контролю эффективности защиты информации от утечки по ST-каналу, относятся (рис. 27):

E_{31} – меры пассивной защиты информации;

E_{32} – меры активной защиты информации;

E_{33} – меры, реализуемые с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации;

E_{34} – меры, реализуемые с целью дополнительных исследований на предмет наличие ST-канала.

Рис. 27. Декомпозиционное представление мероприятий по техническому контролю эффективности защиты информации от утечки по ST-каналу
Fig. 27. Decomposition view of activities for technical control of the effectiveness of data leakage protection via the ST channel

Третий уровень декомпозиции целевой функции «Противодействие утечке информации по ST-каналу» образуется путем детализации действий, выполняемых в процессе реализации мер E_{11}–E_{34}. Соответствующие данному уровню действия следует рассматривать как функции, реализующие указанные меры.

К функциям, реализующим меры по изменению конфигурации электронного оборудования СВТ (меры E_{11}), относятся (рис. 28):

K_{111} – функция замены аппаратных составляющих электронного оборудования СВТ случайным образом;

K_{112} – функция изменения аппаратной конфигурации электронного оборудования СВТ.

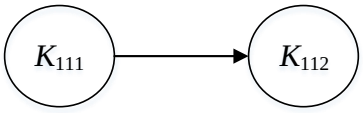

Рис. 28. Декомпозиционное представление мер по изменению конфигурации электронного оборудования СВТ

Fig. 28. Decomposition view of measures to change the configuration of electronic equipment of CT

К функциям, реализующим меры по замене импортного программно-аппаратного обеспечения СВТ на отечественное (меры E_{12}), относятся (рис. 29):

K_{121} – функция замены импортного программного обеспечения на отечественное;

K_{122} – функция замены импортного аппаратного обеспечения на отечественное.

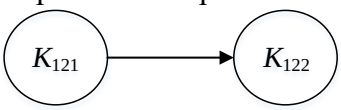

Рис. 29. Декомпозиционное представление мер по замене импортного программно-аппаратного обеспечения СВТ на отечественное

Fig. 29. Decomposition view of measures to replace imported hardware and software with domestic hardware of CT

К функциям, реализующим меры по проведению исследований на соответствие требованиям по безопасности информации (меры E_{21}), относятся (рис. 30):

K_{211} – функция проведения специальных проверок СВТ;

K_{212} – функция проведения специальных исследований СВТ.

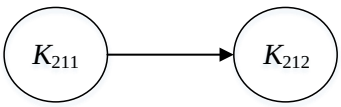

Рис. 30. Декомпозиционное представление мер по проведению исследований на соответствие требованиям по безопасности информации

Fig. 30. Decomposition view of measures to ensure compliance of the research activities with information security requirements

К функциям, реализующим меры по проведению дополнительных исследований (меры E_{22}), относятся (рис. 31):

K_{221} – функция формирования статистического профиля работы СВТ;

K_{222} – функция создания профиля помехи;

K_{223} – функция сравнения статистического профиля работы СВТ с эталонными образцами.

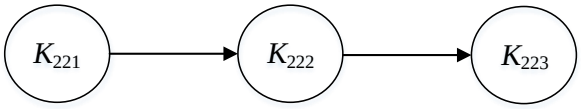

Рис. 31. Декомпозиционное представление мер по проведению дополнительных исследований
Fig. 31. Decomposition view of measures for additional research

К функциям, реализующим меры пассивной защиты информации (меры E_{31}), относятся (рис. 32):

K_{311} – функция полного или частичного экранирования помещения, в котором размещено СВТ;

K_{312} – функция полного или частичного экранирования СВТ.

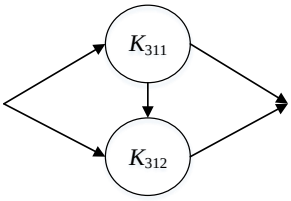

Рис. 32. Декомпозиционное представление мер пассивной защиты информации
Fig. 32. Decomposition view of passive information protection measures

К функциям, реализующим меры активной защиты информации (меры E_{32}), относятся (рис. 33):

K_{321} – функция применения генератора шума широкополосной помехи;

K_{322} – функция применения генератора шума прицельной помехи.

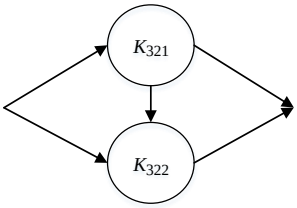

Рис. 33. Декомпозиционное представление мер активной защиты информации
Fig. 33. Decomposition view of active information protection measures

К функциям, реализующим меры, реализуемые с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации (меры E_{33}), относятся (рис. 34):

K_{331} – функция проведения экспертно-документального контроля эффективности защиты информации от утечки по ST-каналу;

K_{332} – функция проведения инструментального контроля эффективности защиты информации от утечки по ST-каналу.

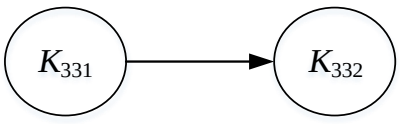

Рис. 34. Декомпозиционное представление мер, реализуемых с целью оценки эффективности защиты информации от утечки по ST-каналу в соответствии требованиями по безопасности информации
Fig. 34. Decomposition view of measures implemented to assess the effectiveness of the information leakage protection via the ST channel in accordance with information security requirements

К функциям, реализующим меры, реализуемые с целью дополнительных исследований на предмет наличие ST-канала (меры E_{34}), относятся (рис. 35):

K_{341} – функция анализа программного обеспечения СВТ на предмет обнаружения фрагментов кода, инициирующего модуляцию;

K_{342} – функция контроля времени работы электронного оборудования СВТ;

K_{343} – функция использования аппаратных верификаторов работы интерфейсов передачи данных электронного оборудования СВТ;

K_{344} – функция периодического контроля статистического профиля работы СВТ.

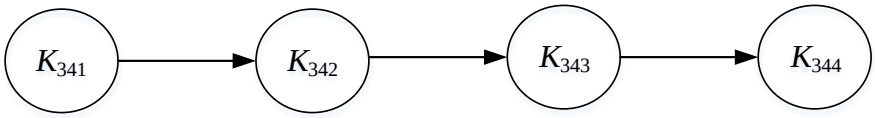

Рис. 35. Декомпозиционное представление мер, реализуемых с целью дополнительных исследований на предмет наличие ST-канала

Fig. 35. Decomposition view of measures implemented to allow additional research on the presence of an ST channel

Заключение

Традиционно в практике технической защиты информации для анализа защищенности объектов информатизации от утечки по техническим каналам разработаны соответствующие методики, основанные на экспертном анализе субъектно-объектных взаимосвязей между источниками угроз утечки информации и ее уязвимостями к такого рода угрозам. При этом данные методики не учитывают те случайные состояния исследуемых процессов, которые характеризуют их динамику.

Функциональное моделирование дает возможность представить случайные состояния процессов перехвата информативных сигналов СВТ по ST-каналу и противодействия утечке информации в терминах Марковских процессов. Подобное представление является предпосылкой для разработки математических моделей временных характеристик рассматриваемого типа угроз и мер реагирования на их проявление, что, в итоге, позволяет количественно оценить эффективность противодействия утечке информации по ST-каналу с учетом динамики его возникновения, продолжительности утечки и проводимых мероприятий по обеспечению защищенности информации. Естественно, что в этих условиях адекватность оценки защищенности информации будет выше адекватности оценки, полученной с помощью существующих методик.

СПИСОК ЛИТЕРАТУРЫ:

1. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. Специальная техника. 2010, № 2, с. 39–57. URL: https://www.elibrary.ru/item.asp?id=15134772 (дата обращения: 20.12.2021).
2. Кузнецов Ю.В., Баев А.Б., Коновалюк М.А., Горбунова А.А. Исследование непреднамеренных электромагнитных излучений средств вычислительной техники. Специальная техника. 2017, № 1, с. 2–15. URL: https://www.elibrary.ru/item.asp?id=29243415 (дата обращения: 20.12.2021).
3. Гончаров Н.И., Сирота А.А., Гончаров И.В. Анализ защищённости сетевых систем обработки данных по отношению к техническим каналам утечки информации. Специальная техника. 2017, № 1, с. 39–47. URL: https://www.elibrary.ru/item.asp?id=29243426 (дата обращения: 20.12.2021).
4. Авдеев В.Б., Анищенко А. В., Петигин А.Ф. Методический подход к оценке защищённости информации, обрабатываемой компьютером с использованием сложных сигналов, от утечки за счёт побочных электромагнитных излучений. Специальная техника. 2017, № 3, с. 40–47. URL: https://www.elibrary.ru/item.asp?id=29368071 (дата обращения: 20.12.2021).

5. Kuhn M.G. and Anderson R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Information Hiding (1998), D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Springer, p. 124–142. DOI: https://doi.org/10.1007/3-540-49380-8_10.
6. Краева Е.В., Татарникова Т.М., Веревкин С.А., Миклуш В.А., Богданов П.Ю., Мартын И.А. Актуальность стеганографии и ее практическое применение. Информационные технологии и системы: управление, экономика, транспорт, право. СПб.: ООО «Андреевский издательский дом». 2019, № 3 (35), с. 105–109. URL: https://www.elibrary.ru/item.asp?id=41880024 (дата обращения: 20.12.2021).
7. Касперский Е.В. Компьютерное zловредство. СПб.: Издательство «Питер». 2007. – 208 с.
8. Markus G. Kuhn. Security Limits for Compromising Emanations (англ.). Cryptographic Hardware and Embedded Systems: журнал. 2005, vol. 3659, p. 265–279. DOI: http://dx.doi.org/10.1007/11545262_20.
9. Guri M.; Kedma G.; Kachlon A.; Elovici Y. (October 2014). AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). P. 58–67. DOI: http://dx.doi.org/10.1109/MALWARE.2014.6999418.
10. Guri, M.; Monitz, M.; Elovici, Y. (December 2016). USBee: Air-gap covert-channel via electromagnetic emission from USB. 2016 14th Annual Conference on Privacy, Security and Trust (PST). P. 264–268. DOI: http://dx.doi.org/10.1109/PST.2016.7906972.
11. Guri M.; Monitz M.; Mirski Y.; Elovici Y. (July 2015). BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. 2015 IEEE 28th Computer Security Foundations Symposium. P. 276–289. DOI: http://dx.doi.org/10.1109/CSF.2015.26.
12. Лиходедов Д.Ю., Волкова С.Н. О некоторых особенностях функционального представления деятельности по защите информации от утечки по техническим каналам. Охрана, безопасность и связь – 2011: материалы Международной научно-практ. конф. Часть 1. Воронеж: Воронежский институт МВД России. 2012, с. 195–198. URL: https://socionet.ru/publication.xml?h=spz:neicon:radioprom:y:2021:i:2:p:22-34&l=en (дата доступа:20.12.2021).
13. Волкова С.Н., Дерябин А.С. Функциональное моделирование, как инструмент исследования механизмов защиты информации. Информация и безопасность. Воронеж: ВГТУ. 2010, Вып. 2, с. 303–304. URL: https://www.elibrary.ru/item.asp?id=15122817 (дата доступа:28.02.2022)
14. Скрыль С.В., Крылов В.О., Филева С.А, Гуляев О.А. Функциональное представление угроз утечки информации по виброакустическим каналам на объектах авиакосмической промышленности. Авиакосмическое приборостроение. М: «Научтехлитиздат». 2017, № 12, с. 22–32. URL: https://www.elibrary.ru/item.asp?id=30740965 (дата доступа:28.02.2022)
15. Ревюз Д. Цепи Маркова / пер. с англ. М.: РФФИ, 1997. – 432 с.
16. Скрыль С.В., Сычев М.П. и др. Направления развития существующей концепции оценки актуальности угроз утечки информации по техническим каналам в условиях современных тенденций совершенствования технической разведки. Радиопромышленность. М: АО «ЦНИИ «Электроника». 2021, т. 31, № 1, с. 74–83. URL: https://www.elibrary.ru/item.asp?id=45540861 (дата обращения: 20.12.2021).

REFERENCES:

[1] Chorev A.A. Technical channels of information leakage processed by computer equipment. Specialnaya Technika. 2010, no.2, p. 39–57. URL: https://www.elibrary.ru/item.asp?id=15134772 (accessed: 20.12.2021) (in Russian).
[2] Kuznetsov Y.V., Bayev A.B., Konovaluk M.A., Gorbunova A.A. Research on unintentional electromagnetic emissions of computer equipment. Specialnaya Technika [Special Technique]. 2017, no. 1, p. 2–15. URL: https://www.elibrary.ru/item.asp?id=29243415 (accessed: 20.12.2021) (in Russian).
[3] Goncharov N.I., Sirota A.A., Goncharov I.V. Analysis of the security of data processing network systems in connection with technical channels of information leakage. Specialnaya Technika [Special Technique]. 2017, no.1, p. 39–47. URL: https://www.elibrary.ru/item.asp?id=29243426 (accessed: 20.12.2021) (in Russian).
[4] Avdeeva V.B., Anischenko A.V., Petigin A.F. A methodological approach to assessing the security of computer-processed information using complex signals from leakage due to transient electromagnetic pulse emanation. Specialnaya Technika [Special Technique]. 2017, no. 3, p. 40–47. URL: https://www.elibrary.ru/item.asp?id=29368071 (accessed: 20.12.2021) (in Russian).
[5] Kuhn M.G. and Anderson, R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Information Hiding (1998), D. Aucsmith, Ed., vol. 1525 of Lecture Notes in Computer Science, Springer, p. 124–142. DOI: https://doi.org/10.1007/3-540-49380-8_10.

[6] Krayeva E.V., Tatarnikova T.M., Verevkin S.A., Mikluch V.A., Bogdanov P.Y., Martyn I.A. The relevance of steganography and its practical application. Informatsionnie technologii I sistemi: upravlenie, economika, transport, pravo [Information technology and systems: management, economics, transport, law.], Saint-Petersburg, Andreevskii izdatelskiy dom Publ. 2019, no. 3 (35), p. 105–109. URL: https://www.elibrary.ru/item.asp?id=41880024 (accessed: 20.12.2021) (in Russian).

[7] Kaspersky E.V. Komputernoe zlovredstvo [Computer malware.], Saint-Petersburg, Piter Publ. 2007. – 208 p. (in Russian).

[8] Markus G. Kuhn. Security Limits for Compromising Emanations. Cryptographic Hardware and Embedded Systems: журнал. 2005, vol. 3659, p. 265–279. DOI: http://dx.doi.org/10.1007/11545262_20.

[9] Guri M.; Kedma G.; Kachlon A.; Elovici Y. (October 2014). AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). P. 58–67. DOI: http://dx.doi.org/10.1109/MALWARE.2014.6999418.

[10] Guri, M.; Monitz, M.; Elovici, Y. (December 2016). USBee: Air-gap covert-channel via electromagnetic emission from USB. 2016 14th Annual Conference on Privacy, Security and Trust (PST). P. 264–268. DOI: http://dx.doi.org/10.1109/PST.2016.7906972.

[11] Guri M.; Monitz M.; Mirski Y.; Elovici Y. (July 2015). BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations. 2015 IEEE 28th Computer Security Foundations Symposium. P. 276–289. DOI: http://dx.doi.org/10.1109/CSF.2015.26.

[12] Likhodedov D.Yu., Volkova S.N. On some features of the functional representation of activities to protect information from leakage through technical channels. Protection, security and communication – 2011: materials of the international scientific and practical. conf. Part 1. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia. 2012, p. 195–198. URL: https://socionet.ru/publication.xml?h=spz:neicon:radioprom:y:2021:i:2:p:22-34&l=en (accessed:20.12.2021) (in Russian).

[13] Volkova S.N., Deryabin A.S. Functional modeling as a tool for studying the mechanisms of information protection. Information and security. Voronezh: VSTU. 2010, Issue. 2, p. 303–304. URL: https://www.elibrary.ru/item.asp?id=30740965 (accessed:28.02.2022) (in Russian).

[14] Skryl S.V., Krylov V.O., Fileva S.A., Gulyaev O.A. Functional representation of threats of information leakage through vibroacoustic channels at objects of the aerospace industry. Aerospace instrumentation. Moscow: «Nauchtekhlitizdat». 2017, no. 12, p. 22–32. URL: https://www.elibrary.ru/item.asp?id=15122817 (accessed:28.02.2022) (in Russian).

[15] Revuz D. Markov Chains. per. from English - M.: RFBR, 1997. – 432 p. (in Russian).

[16] Skryl S.V., Sychev M.P. et al. Directions for the development of the existing concept of assessing the relevance of information leakage threats through technical channels in the context of modern trends in improving technical intelligence. Radio industry. M: JSC "Central Research Institute" Electronics ". 2021, v. 31, no. 1, p. 74–83. URL: https://www.elibrary.ru/item.asp?id=45540861 (accessed: 20.12.2021) (in Russian).

Поступила в редакцию – 27 декабря 2021 г. Окончательный вариант – 05 февраля 2022 г.
Received – December 27, 2021. The final version – February 05, 2022.