А. О. Авсентьев,
кандидат технических наук

А. Г. Кругов

В. Н. Пржегорлинский,
кандидат технических наук, доцент

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ РЕАЛИЗАЦИИ ПРОЦЕССОВ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

FUNCTIONAL MODEL OF IMPLEMENTATION OF PROCESSES FOR PROTECTING VOICE INFORMATION FROM LEAKAGE DUE TO SIDE ELECTROMAGNETIC RADIATION OF INFORMATIZATION OBJECTS

Рассматривается методический аппарат построения функциональной модели процесса защиты речевой информации в условиях параллельной и асинхронной реализации разнородных процессов ее передачи в объекте информатизации, утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений объекта, используемый в качестве инструмента предварительной формализации исследуемых процессов для их последующего представления в виде полумарковских парциальных процессов с целью преобразования разработанных моделей в математические с использованием аппарата составных сетей Петри — Маркова.

The article considers the methodological apparatus for constructing a functional model of the process of protecting speech information in the conditions of parallel and asynchronous implementation of heterogeneous processes of its transmission in the object of informatization, leakage through technical channels arising from side electromagnetic radiation of the object, which is used as a tool for preliminary formalization of the processes under study for their subsequent presentation in the form of semi-Markov partial processes in order to transform the developed models into mathematical ones using the apparatus of composite Petri — Markov nets.

Введение. В соответствии с положениями существующего методического обеспечения защиты информации в объектах информатизации (ОИ) государственного значения, содержащих информацию, не составляющую государственной тайны, первоначальными процедурами решения различных задач, связанных с исследованием характеристик информационных процессов (*Ipr*) как объекта защиты, процессов реализации угроз безопасности информации (*Pru*) [1], а также задач разработки моделей защиты этой информации, является выявление закономерностей практики формирования системы защиты информации (СЗИ). В настоящее время выбор мер защиты и формирование СЗИ осуществляются на основе базового набора мер [2], а также опыта экспертов в данной предметной области. Несмотря на то, что в составе базовых наборов мер защиты информации (БНМЗИ) в ОИ практически отсутствуют меры защиты от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений (ПЭМИ), нормативным документом [1] предусмотрены процедуры адаптации выбранного БНМЗИ применительно к конкретному ОИ, уточнения и дополнения этого набора мер с учетом

структурно-функциональных характеристик объекта, применяемых информационных технологий, дополнительных требований иных нормативных, а также ведомственных руководящих документов. При этом оцениваются возможности реализации нарушителем различных УБИ, в том числе угроз ее утечки по техническим каналам рассматриваемого типа, а также необходимость включения в состав СЗИ соответствующих мер защиты от утечки. Однако в связи с особенностями реализации нарушителем перехвата информации по техническим каналам ее утечки возникает необходимость исследования условий реализации такого перехвата и обоснования используемого для оценки защищенности этой информации от утечки методического аппарата. В настоящее время требования к защите информации от утечки по техническим каналам, возникающим за счет ПЭМИ РЭУ ОИ государственного значения, определены в нормативном документе ФСТЭК России [3]. При этом в качестве методического обеспечения для реализации защиты применяются инструментально-расчетные методики, направленные на измерение энергетических параметров ПЭМИ в непосредственной близости от структурных элементов ОИ, содержащих в своем составе РЭУ, которые могут выступать в качестве источника (датчика) информации для технического канала утечки информации (ТКУИ), воздействующей на эти РЭУ. На основании этих измерений производятся расчеты требуемых для обеспечения защиты информации размеров контролируемой зоны (КЗ) вокруг ОИ и делается вывод о необходимости применения мер защиты. Как показано в [4, 5], указанные методики являются неточными и их применение приводит, как правило, к завышенным оценкам защищенности информации от утечки по ТКУИ рассматриваемого типа. Кроме того, при этом учитываются лишь условия распространения ПЭМИ и не учитываются характеристики применяемого нарушителем технического средства (ТС) для их перехвата, временные характеристики его действий по реализации ТКУИ, время реализации процесса *Ipr* (время существования информации) в ОИ, а также совокупность функций, выполняемых в ходе реализации процесса защиты информации (*Prz*). Указанные обстоятельства обусловливают невозможность учета взаимосвязей и динамики параллельно и асинхронно реализуемых процессов *Ipr*, *Prz* и *Prz* с применением этих методик.

Это связано с тем, что выполнение энергетических условий, при которых у нарушителя имеется возможность перехвата ПЭМИ РЭУ ОИ, не означает, что он успеет их перехватить при помощи ТС и в них содержится информация, представляющая для нарушителя интерес. Кроме того, возможности реализации перехвата определяются рядом факторов: наличие РЭУ в составе ОИ, которые могут выступать в качестве датчиков ПЭМИ, обрабатываемой в ОИ и перехватываемой нарушителем информации; обеспечение за пределами КЗ объекта условий распространения этих ПЭМИ, при которых возможно применение ТС их перехвата, имеющих необходимый уровень чувствительности; наличие условий для скрытного выполнения нарушителем действий по применению этих ТС. При этом противодействие перехвату информации становится возможным за счет применения организационно-технических мер ее защиты превентивного характера [6, 7], направленных на блокирование действий нарушителя по реализации *Pru*.

Динамика реализации каждого из рассматриваемых процессов характеризуется их вероятностно-временными характеристиками, включающими случайные времена начала, продолжительности и завершения реализации. Это обусловливает сложность учета этих характеристик при оценке защищенности информации в ОИ от утечки по ТКУИ, возникающим за счет ПЭМИ РЭУ, с целью выбора соответствующих мер защиты. При этом задача оценки защищенности информации от утечки может быть решена только на основе методов количественной оценки с разработкой соответствующей математической модели.

В связи с тем, что каждый из рассматриваемых процессов в отдельности может быть представлен в виде последовательности действий, выполняемых во времени, а их

реализации в этом случае обладают всеми признаками марковских процессов, то в интересах учета фактора времени для оценки временных характеристик этих процессов может быть использован аппарат марковских, а в случае параллельной реализации некоторых из этих действий — аппарат полумарковских процессов [8, 9]. Однако наличие взаимосвязей между этими процессами, асинхронность и параллельность реализации некоторых последовательностей действий, их составляющих, а также различных логических условий обусловливает существенные трудности учета динамики такой реализации. В качестве такого рода условий следует рассматривать следующие: 1) процесс *Pru* может быть реализован тогда, когда в ОИ реализуется процесс *Ipr*, то есть в ОИ содержится подлежащая защите информация; 2) в составе ОИ имеются РЭУ, которые проявляют чувствительность к информационным сигналам, воздействующим на их вход, и формируют на выходе отклик в виде информативных ПЭМИ с энергетическими характеристиками, позволяющими выявлять содержание сообщения [10]; 3) это сообщение содержит нужные нарушителю сведения; 4) им подготовлено к работе и настроено ТС перехвата ПЭМИ и т.д.

Процесс *Prz* может быть реализован за счет применения СЗИ, сформированной предварительно как независимо от реализации *Pru*, так и с применением дополнительных превентивных мер защиты с учетом реализации нарушителем процесса перехвата информации по ПЭМИ РЭУ ОИ.

В этих условиях аналитически учесть временной фактор с применением математических моделей на основе традиционных аппаратов марковских и полумарковских процессов практически невозможно. В [11, 12] для аналитического расчета показателей оценки эффективности защиты информации в информационных системах электронного документооборота было предложено применять аппарат сетей Петри — Маркова, позволяющий моделировать процессы рассматриваемого типа с учетом динамики их реализации и при наличии различных логических условий. Однако, как показано в [13], для применения этого аппарата в интересах моделирования процесса *Prz* целесообразно предварительно разработать функциональные модели, включающие совокупности действий (функций), выполняемых при реализации процессов *Ipr*, *Pru*, в условиях реализации процесса *Prz*, направленного на пресечение выполнения нарушителем действий по реализации перехвата информации по ПЭМИ. С учетом взаимосвязей и динамики реализации этих процессов в качестве цели защиты рассматривается своевременное реагирование СЗИ на действия нарушителя по реализации *Pru*.

В данной работе в качестве примера рассматривается методический аппарат построения функциональной модели процесса защиты речевой информации в условиях параллельной и асинхронной реализации разнородных процессов *Ipr*, *Pru* в интересах ее использования для разработки математической модели этих процессов.

Описание процесса защиты речевой информации от утечки за счет побочных электромагнитных излучений радиоэлектронных устройств объекта информатизации. При описании процессов защиты речевой информации, содержащей сведения конфиденциального характера, в условиях реализации нарушителем угроз ее утечки за счет ПЭМИ РЭУ ОИ учитывались следующие условия.

1. В качестве ОИ рассматривался объект, представляющий собой выделенное помещение (конференц-зал), оборудованное средствами звукоусиления, звукозаписи, звуковоспроизведения, видео-усиления, средствами отображения графических изображений (компьютер, проектор, компьютерные мониторы).

2. Мероприятия, при проведении которых возможен обмен конфиденциальной речевой информацией, могут начинаться в произвольные (для нарушителя) моменты времени и иметь различную продолжительность в течение рабочего дня. Процесс *Ipr* считается случайным во времени.

3. Перед началом мероприятия операторы ОИ выполняют процедуры (действия) по подготовке оборудования к работе в заданном режиме. Время подготовки оборудования к работе также является случайной величиной. Оборудование функционирует до окончания мероприятия.

4. Сведения конфиденциального характера могут содержать отдельные фрагменты продолжительности речевых сообщений различных участников мероприятия. Временные характеристики (начало, продолжительность и окончание) таких фрагментов являются случайными.

5. Нарушитель осуществляет перехват речевой информации по ПЭМИ скрытно с применением портативного приемника ТС (сканерного приемника) на территории, прилегающей к КЗ ОИ. В связи с этим время возможной реализации процесса *Pru* является случайным и ограничено условиями обеспечения скрытности.

6. Перед перехватом речевой информации нарушитель выполняет ряд процедур (действий): 1) обнаружение ПЭМИ РЭУ путем сканирования частотного диапазона в течение времени, зависящего от технических характеристик применяемого ТС; 2) определение направления максимального уровня излучения ПЭМИ [14]; 3) выбор места применения ТС с обеспечением условий скрытности и максимального уровня ПЭМИ; 4) определение вида модуляции информативного сигнала ПЭМИ и его частотных характеристик; 5) настройка режима работы ТС применительно к виду перехватываемой информации [13]. Времена выполнения указанных действий зависят от множества факторов: характеристик территории, прилегающей к КЗ (протяженность вдоль границ КЗ и расстояния от этих границ, вид застройки, наличие естественных укрытий и других), тактико-технических характеристик приемника ТС, используемого для реализации перехвата ПЭМИ (скорость сканирования частотного диапазона, виды модуляции принимаемых сигналов, чувствительность, полоса пропускания, наличие направленных антенн). В этих условиях указанные времена являются случайными величинами.

7. В качестве датчика информации, как источника ПЭМИ, на излучение которого настраивается приемник ТС, нарушитель может использовать один из многих РЭУ ОИ.

8. Для защиты речевой информации от утечки по ПЭМИ могут быть применены организационные и технические меры [13] превентивного характера. К организационным мерам относится применение мобильных групп быстрого реагирования (ГБР) — патрульных групп в составе 2-3 человек, осуществляющих патрулирование территории, прилегающей к КЗ ОИ, под управлением администратора СЗИ. Администратор контролирует оперативную обстановку на этой территории с применением систем видеонаблюдения. ГБР осуществляют осмотр территории с целью выявления действий нарушителя и обнаружения места применения им приемника ТС для перехвата ПЭМИ. К техническим мерам относятся применение патрульными ГБР мобильных генераторов шума радиочастотного диапазона и мобильных устройств, имитирующих ложные ПЭМИ.

9. Защита обеспечивается как за счет самого факта появления ГБР на территории, прилегающей к КЗ, с целью пресечения перечисленных действий нарушителя и его удаления с этой территории, так и за счет применения технических средств активной защиты с целью подавления канала утечки. Защита может быть обеспечена при условии, что указанные организационные и технические меры будут опережать выполнение соответствующих действий нарушителем [11].

Условие 1 характеризует обширность номенклатуры ОИ и характеристик ПЭМИ их структурных элементов, содержащих в своем составе различного рода РЭУ.

Условия 2, 3 и 4 характеризуют динамику реализации процесса *IPr*. Общее время τ_{IPr} его реализации включает время τ_{eq} подготовки оборудования к работе, время τ_{exp} ожидания начала мероприятия, времена $\tau_{dur}^{(n)}, n = \overline{1, N}$ продолжительностей сообщений

его участников и является случайным со средним значением $\overline{\tau}_{IPr} = \overline{\tau}_{eq} + \overline{\tau}_{exp} + \sum_{n=1}^{N} \overline{\tau}_{dur}^{(n)}$, где $\overline{\tau}_{eq}, \overline{\tau}_{exp}, \overline{\tau}_{dur}^{(n)}$ — средние значения случайных величин $\tau_{eq}, \tau_{exp}, \tau_{dur}^{(n)}$, соответственно. Кроме того, в соответствии с условием 4 только в течение $\delta \cdot \tau_{IPr}$ части общего времени реализации процесса *IPr* может содержаться конфиденциальная информация.

Условия 5—7 характеризуют динамику реализации процесса *Pru* перехвата речевой информации. Общее время τ_{Pru} реализации процесса *Pru*, как случайная величина, характеризуется его средним значением $\overline{\tau}_{Pru} = \left(\overline{\tau}_{det} + \overline{\tau}_{dir} + \overline{\tau}_{pl} + \overline{\tau}_{ch} + \overline{\tau}_{mod}\right) + \overline{\tau}_{int}$, где $\overline{\tau}_{det}, \overline{\tau}_{dir}, \overline{\tau}_{pl}, \overline{\tau}_{ch}, \overline{\tau}_{mod}$, $\overline{\tau}_{int}$ — средние значения случайных времен τ_{det}, τ_{dir}, τ_{pl}, τ_{ch}, τ_{mod}, выполнения нарушителем действий, обозначенных в подпунктах 1)—5), соответственно, условия 6, и среднее значение случайного времени перехвата информации τ_{int}. Условие 7 означает возможность наличия ПЭМИ нескольких РЭУ, имеющих различные характеристики. Нарушитель имеет возможность выбора наиболее приемлемого для реализации *Pru*.

Условие 8 характеризует динамику реализации процесса *Prz* защиты информации. Случайные времена выполнения превентивных мер защиты направлены на пресечение выполнения нарушителем действий по реализации *Pru*, указанных в подпунктах 1—5, условия 6 соответственно, τ_{det}^{sup}, τ_{dir}^{sup}, τ_{pl}^{sup}, τ_{ch}^{sup}, τ_{mod}^{sup}, τ_{int}^{sup} и характеризуются их средними значениями: $\overline{\tau}_{det}^{sup}$, $\overline{\tau}_{dir}^{sup}$, $\overline{\tau}_{pl}^{sup}$, $\overline{\tau}_{ch}^{sup}$, $\overline{\tau}_{mod}^{sup}$, $\overline{\tau}_{int}^{sup}$.

Условие 9 характеризует защищенность информации по показателю опережения мерами защиты реализации угрозы утечки речевой информации за счет ПЭМИ РЭУ ОИ в соответствии с условием

$$\overline{\tau}_{int} < \delta \cdot \overline{\tau}_{IPr}. \tag{1}$$

Это фактически означает, что процесс реализации угрозы за счет применения превентивных мер защиты либо пресекается при выполнении нарушителем действий на любом из подготовительных этапов, определенных подпунктами 1—5 условия 6, либо за счет увеличения общего времени τ_{prep} подготовки приемника ТС к перехвату, включающего случайные времена τ_{det}, τ_{dir}, τ_{pl}, τ_{ch}, τ_{mod}, до величин, при которых временной объем перехваченной информации не удовлетворяет требованиям нарушителя:

$$\overline{\tau}_{prep} > \left(\overline{\tau}_{Ipr} - \delta \cdot \overline{\tau}_{IPr}\right). \tag{2}$$

При этом не учитывается, в выступлении какого (или каких) из участников мероприятия содержатся сведения конфиденциального характера (условие 4).

Вероятность выполнения условий (1) и (2) определим в качестве показателей оценки защищенности речевой информации от утечки по техническим каналам, возникающим за счет ПЭМИ РЭУ ОИ:

$$\eta_{zi} = P\left(\tau_{int} < \delta \cdot \tau_{IPr}\right), \tag{3}$$

$$\eta_{zi} = P\left(\tau_{prep} > \left(\tau_{Ipr} - \delta \cdot \tau_{IPr}\right)\right). \tag{4}$$

Учет условия (4) возможен только на основе количественных оценок с разработкой соответствующих математических моделей.

В соответствии с условием 1 невозможно разработать единое описание процесса реализации угроз утечки речевой информации за счет ПЭМИ РЭУ ОИ, имеющих различное назначение и структурно-функциональные характеристики. Для каждого объекта и применяемых мер защиты информации необходимо формировать свою описательную модель. Это обусловлено существенными различиями в содержании и последовательно-

сти действий нарушителя, выполняемых им в различных условиях на территории, прилегающей к КЗ объекта, в применении для реализации такого рода угроз приемников ТС, имеющих различные характеристики, в необходимости учета применения легитимными пользователями объекта различных штатных и превентивных мер защиты.

Содержание описательных моделей процессов реализации угроз утечки речевой информации по техническим каналам за счет ПЭМИ РЭУ ОИ служит основой для разработки функциональных моделей этих процессов, которые, в свою очередь, используются при разработке математических моделей оценки защищенности речевой информации, содержащейся в ОИ, от утечки по техническим каналам рассматриваемого типа.

Функциональное представление процессов защиты речевой информации от утечки по техническим каналам за счет побочных электромагнитных излучений радиоэлектронных устройств объекта информатизации. Формально с учетом условий 1—9 функциональная модель процесса защиты речевой информации в условиях реализации нарушителем ее перехвата по техническим каналам рассматриваемого типа может быть представлена в виде совокупности трех параллельно реализуемых взаимосвязанных указанными условиями процессов *Ipr*, *Pru*, *Prz*, каждый из которых, в свою очередь, представляется совокупностью трех множеств [15]:

$$\Phi_i^{Ipr} = \left\{ D_i^{Ipr}, M(D_i^{Ipr}), Y(D_i^{Ipr}) \right\}, i = \overline{1, I}, \quad (5)$$

где D_i^{Ipr} — множество действий (функций), которые нужно выполнить для реализации *i*-го варианта *Ipr*, *I* — мощность множества D_i^{Ipr};

$M(D_i^{Ipr})$ — матрица взаимосвязей действий, отражающая порядок их выполнения;

$Y(D_i^{Ipr})$ — совокупность условий успешного выполнения этих действий (условия 1—4), при которых возможна реализация *i*-го варианта реализации *Ipr*.

$$\Phi_j^{Pru} = \left\{ D_j^{Pru}, M(D_j^{Pru}), Y(D_j^{Pru}) \right\}, j = \overline{1, J}, \quad (6)$$

где D_j^{Pru} — множество действий (функций), выполняемых при реализации *j*-го варианта *Pru*, *J* — мощность множества D_j^{Pru};

$M(D_j^{Pru})$ — матрица взаимосвязей действий, отражающая порядок их выполнения;

$Y(D_j^{Pru})$ — совокупность условий успешного выполнения этих действий (условия 5—7), при которых возможна реализация *j*-го варианта реализации *Pru*.

$$\Phi_k^{Prz} = \left\{ D_k^{Prz}, M(D_k^{Prz}), Y(D_k^{Prz}) \right\}, k = \overline{1, K}, \quad (7)$$

где D_k^{Prz} — множество действий (функций), выполняемых при реализации *k*-го варианта *Prz*, *K* — мощность множества D_k^{Prz};

$M(D_k^{Prz})$ — матрица взаимосвязей действий, отражающая порядок их выполнения;

$Y(D_k^{Prz})$ — совокупность условий успешного выполнения этих действий (условия 8, 9), при которых возможна реализация *k*-го варианта реализации *Prz*.

С учетом представлений (5) — (7) разработана функциональная модель защиты информации, содержащейся в ОИ, в условиях реализации нарушителем процесса ее перехвата по ТКУИ, возникающим за счет ПЭМИ РЭУ объекта, включающая совокупности подлежащих выполнению действий по реализации процессов *Ipr*, *Pru* и *Prz*, взаимосвязей этих действий и условий 1—9 их выполнения, представленная на рисунке. С целью упрощения индексации действий, выполняемых в интересах реализации различных процессов, на рисунке использована общая индексация, а принадлежность действий в соответствии с представлениями (5) — (7) определена в их обозначениях.

На рисунке используются следующие обозначения действий d_1—d_{24}:

d_1 — включение, тестирование и перевод системы звукоусиления в режим ожидания;

d_2 — звукоусиление речи выступающего, сопровождающееся появлением ПЭМИ;

d_3 — звукоусиление выступления участника совещания;

d_4 — осмотр территории группой быстрого реагирования с целью обнаружения нарушителей;

d_5 — наблюдение за территорией со стороны ГБР с целью обнаружения нарушителя;

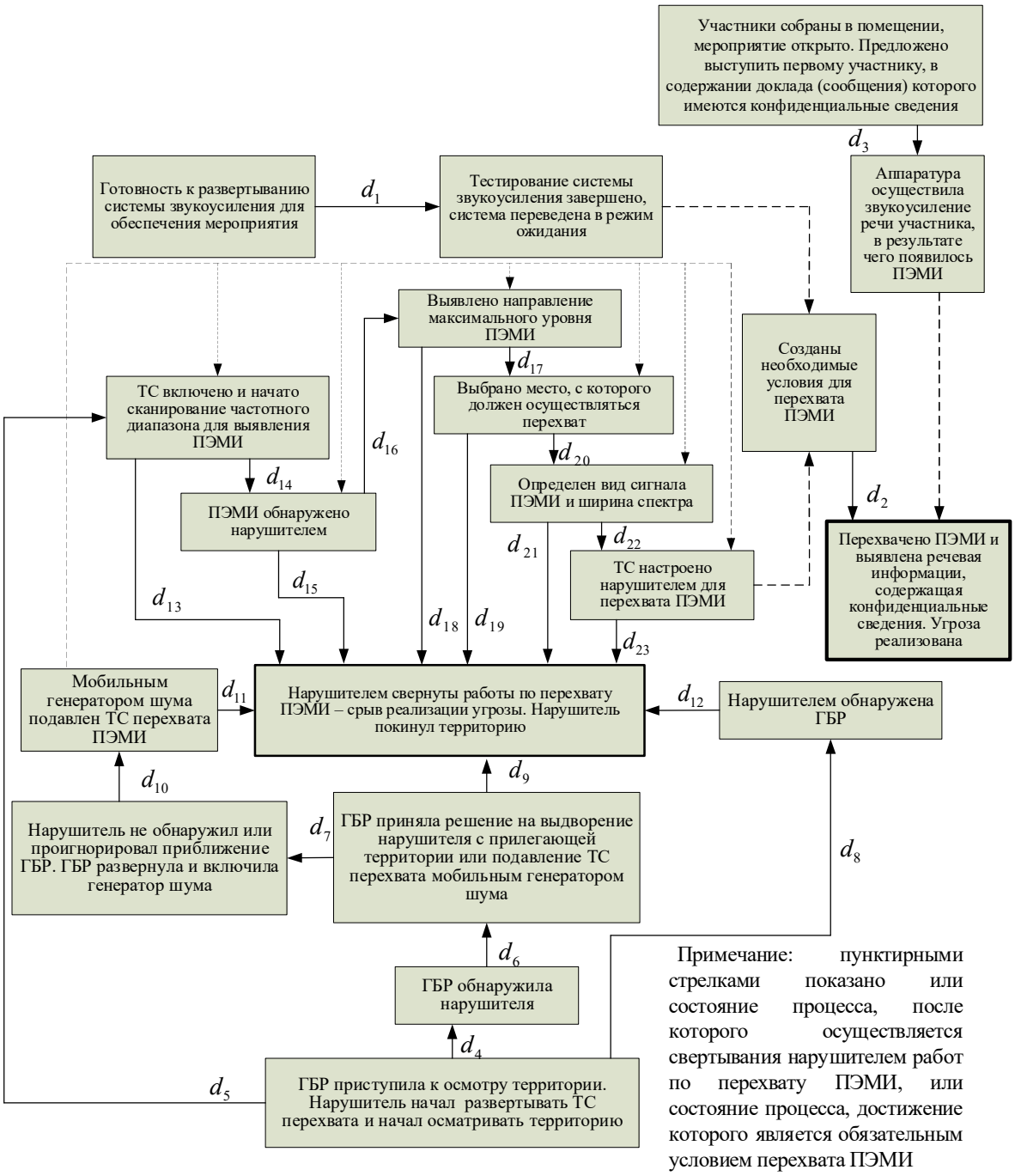
d_6 — наблюдение приближение ГБР к нарушителю. Принятие решения на выдворение нарушителя с территории или подавление его ТС;

d_7 — развертывание мобильного генератора шума;

d_8 — обнаружение нарушителем патрульной группы;

d_9 — выдворение нарушителя патрульной группой;

d_{10} — подавление ТС перехвата мобильным генератором шума;



Функциональная модель процесса перехвата речевой информации по побочным электромагнитным излучениям радиоэлектронных устройств объекта информатизации

d_{11} — выявление нарушителем факта подавления ТС перехвата и свертывание работ по перехвату ПЭМИ;

d_{12} — свертывание работ после обнаружения патрульной группы;

d_{13} — свертывание работ в ходе сканирования частотного диапазона;

d_{14} — обнаружение нарушителем ПЭМИ в ходе сканирования частотного диапазона;

d_{15} — свертывание работ после завершения сканирования частотного диапазона;

d_{16} — выявление нарушителем направления максимального уровня ПЭМИ;

d_{17} — поиск места, с которого должен осуществляться перехват;

d_{18} — свертывание работ по перехвату ПЭМИ в ходе или после определения максимального уровня ПЭМИ из-за появления ГБР или подавления;

d_{19} — свертывание работ по перехвату ПЭМИ в ходе или после выбора места, с которого должен осуществляться перехват, из-за появления ГБР или подавления;

d_{20} — определение вида сигнала ПЭМИ и ширины спектра;

d_{21} — свертывание работ в ходе или после определения вида сигнала ПЭМИ и ширины его спектра;

d_{22} — настройка нарушителем ТС для перехвата ПЭМИ с речью участника мероприятия;

d_{23} — свертывание работ в ходе или после настройки нарушителем ТС перехвата;

d_{24} — осуществление перехвата ПЭМИ с записью речевой информации.

Как показано на рисунке, ряд действий, выполняемых в интересах реализации одного и того же процесса, осуществляются последовательно одно за другим. Однако некоторые из таких последовательностей представляют композицию действий, выполняемых параллельно и независимо одно от другого. Это обстоятельство обусловливает существенные трудности при оценке общего времени реализации процессов рассматриваемого типа. В связи с этим функциональные модели используются для предварительной формализации исследуемых процессов в интересах разработки аналитических моделей для такой оценки.

Заключение. Представленная функциональная модель по аналогии с [12] может служить основой для разработки с использованием аппарата сетей Петри — Маркова [18] аналитической модели динамики реализации процесса защиты речевой информации от угроз ее утечки по техническим каналам, возникающим за счет ПЭМИ РЭУ ОИ, учитывающей вероятностно-временные характеристики действий нарушителя, выполняемых последовательно-параллельно и при наличии различных логических условий, адекватно отражающей процессы реализации перехвата информации, содержащейся в конкретном ОИ, и позволяющей получить аналитические соотношения для расчета показателей защищенности информации от утечки как без применения, так и в условиях применения превентивных мер защиты.

ЛИТЕРАТУРА

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17 [Электронный ресурс]. — URL: https://base.garant.ru/70391358.

2. Меры защиты информации в государственных информационных системах : методический документ: утв. ФСТЭК России 11 февраля 2014 г. — URL: fstec.ru

3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) : утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.

4. Авдеев В. Б., Катруша А. Н. Расчёт коэффициента ослабления побочных электромагнитных излучений // Специальная техника. — 2013. — № 2. — С. 18—27.

5. Авдеев В. Б., Анищенко А. В. Сравнительная оценка методических подходов к расчёту отношения сигнал/шум в задачах контроля защищённости информации от утечки за счёт побочных электромагнитных излучений // Специальная техника. — 2016.

— № 1. — С. 54—63.

6. Хорев А. А. Техническая защита информации : учеб. пособие для студентов вузов : в 3 т. — Т. 1: Технические каналы утечки информации / под ред. Ю. Н. Лаврухина. — М. : Аналитика, 2008. — 436 с.

7. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. Технические средства и методы защиты информации : учебник для вузов. — 7-е изд., испр. — М. : Горячая линия — Телеком, 2012. — 442 с.

8. Тихонов В. И., Миронов М. А. Марковские процессы. — М. : Советское радио, 1977. — 488 с.

9. Иванов Н. Н. Полумарковские процессы во временных стохастических сетях Петри // Автоматика и телемеханика. — 1994. — № 3. — С.117—127.

10. Меньшаков Ю. К. Теоретические основы технических разведок : учеб. пособие / под ред. Ю. Н. Лаврухина. — М. : Изд-во МГТУ им. Н. Э. Баумана, 2008. — 536 с.

11. Авсентьев О. С., Рубцова И. О., Язов Ю. К. К вопросу об оценке эффективности защиты информации в системах электронного документооборота // Вопросы кибербезопасности. — 2019. — № 1(29). — С. 25—34.

12. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри — Маркова / О. С. Авсентьев [и др.] // Труды СПИИРАН. — 2019. — Т. 18. — № 6. — С. 1269—1300

13. Авсентьев А. О., Кругов А. Г., Перова Ю. П. Функциональные модели защиты информации от утечки за счет побочных электромагнитных излучений объектов информатизации / // Доклады ТУСУР. — 2020. — Т. 22. — № 2. — С. 29—39.

14. Антипов Д. А., Шелупанов А. А. Исследование направленности побочного электромагнитного излучения от персонального компьютера // Доклады ТУСУР. — 2018. — № 2. — С. 33—37.

15. Авсентьев О. С., Кругов А. Г., Шелупанова П. А. Функциональные модели процессов реализации угроз утечки информации за счет побочных электромагнитных излучений объектов информатизации // Доклады ТУСУР. — 2020. — Т. 23. — № 1. — С. 29—39.

16. Авсентьев О. С., Авсентьев А. О., Рубцова И. О. Функциональные модели процессов реализации угроз электронному документообороту // Вестник ВИ МВД России. — 2019. — № 4. — С. 40—50.

17. Язов Ю. К., Анищенко А. В. Сети Петри — Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. — Воронеж : Кварта, 2020. — 173 с.