УДК 004.056:519.1

А.О. Авсентьев, А.Г. Кругов, Ю.П. Перова

Функциональные модели защиты информации от утечки за счет побочных электромагнитных излучений объектов информатизации

Рассматривается подход к построению функциональных моделей защиты информации от утечки за счет побочных электромагнитных излучений структурных элементов объектов информатизации, учитывающий динамику параллельно реализуемых процессов перехвата нарушителем этой информации и ее защиты легитимными пользователями от перехвата в условиях применения адаптивных мер защиты, основанный на стратифицированном представлении совокупностей действий, выполняемых при реализации этих процессов.

Ключевые слова: функциональная модель, свойства информации, ценность информации, технический канал утечки информации, адаптивные меры защиты информации, электрические характеристики радиоэлектронных устройств, побочные электромагнитные излучения, условия согласования разнородных характеристик.

doi: 10.21293/1818-0442-2020-23-2-17-35

Объект информатизации (ОИ) в соответствии с его определением, приведенным в [1], может рассматриваться как организационно-техническая система, обеспечивающая процесс передачи, приема, обработки и хранения информации с использованием информационных систем (ИС) как на основе различного рода технических средств, в том числе на основе средств вычислительной техники, так и без использования таких средств в выделенных помещениях. Такие ОИ широко применяются в различных государственных, коммерческих и других структурах. Циркулирующая в их ИС информация может представлять интерес для многих заинтересованных сторон. В этих условиях все более востребованным на практике становится обеспечение безопасности этой информации от угроз нарушения ее конфиденциальности, целостности и доступности.

При этом одной из основных угроз является утечка информации за счет перехвата нарушителем информативных сигналов побочных электромагнитных излучений (ПЭМИ) от основных технических средств и систем (ОТСС) ОИ, приводящая к нарушению ее конфиденциальности [2]. Обеспечение эффективного противодействия угрозам утечки информации ОИ за счет ПЭМИ связано с необходимостью тщательного анализа характеристик структурных элементов (СЭ) объектов и возможностей реализации нарушителем противоправных действий по перехвату информативных сигналов ПЭМИ в условиях ограниченных возможностей применяемых мер защиты информации [3].

В настоящее время в документах государственных регуляторов отсутствуют требования к ОИ рассматриваемого типа в части защиты информации от утечки за счет ПЭМИ. Действующие нормативные документы ФСТЭК России регламентируют требования к ИС в целом или к АИС на основе СВТ. В этих требованиях не учитываются особенности СЭ ОИ и динамика реализации нарушителем противоправных действий по перехвату информативных сигналов ПЭМИ. В частности, в них не учитывается динамика реализации нарушителем процессов перехвата информации по техническим каналам ее утечки (ТКУИ) в рамках реализуемой стратегии технической разведки (ТР), включающей выбор технического средства разведки (ТСР) и места его применения. Учет указанной динамики может не только существенно повлиять на защищенность информации от утечки, но и изменить требования по защите.

Однако для такого учета необходимы математические модели, учитывающие как динамику реализации процессов передачи, приема и обработки информации на ОИ различного типа, так и динамику выполнения нарушителем противоправных действий по ее перехвату. До настоящего времени такие модели для ОИ рассматриваемого типа не разрабатывались, а существующие математические модели защиты информации не учитывают особенностей функционирования различных ОИ и динамику реализации указанных информационных процессов.

С учетом изложенного данная статья, посвященная разработке вербальных и функциональных моделей защиты информации от утечки за счет ПЭМИ СЭ ОИ как средств первичной формализации исследуемых процессов в условиях динамики их реализации, в интересах построения математических моделей оценки защищенности информации ОИ от утечки является актуальной.

Общее описание реализации процессов передачи информации на ОИ и ее перехвата за счет ПЭМИ РЭУ ОИ

Важным аспектом развития методологии оценки защищенности информации ОИ от утечки по техническим каналам за счет ПЭМИ СЭ ОИ является то, что в соответствии с описаниями как канала передачи информации между легитимными пользователями, так и ТКУИ [4], называемыми в [5] основным и побочным, соответственно, эти каналы представляют собой совокупность источника, получателя информации и среды распространения информационного / информативного сигнала. Основное отличие этих каналов состоит в противоположности целей их реализации [5]. При этом обеспечение свойств информации,

как передаваемой, так и перехватываемой по основному и побочному каналам, соответственно, зависит с одной стороны, от электрических характеристик используемых сигналов как материальных носителей этой информации, с другой – от характеристик СЭ соответствующих каналов. Обеспечение свойств передаваемой / перехватываемой информации определяется степенью согласования этих СЭ между собой [6]. Условия согласования указанных характеристик в каналах различного назначения существенно отличаются. По своей сути они представляют собой совокупность действий, выполняемых во времени последовательно-параллельно при наличии разнообразных логических условий их выполнения [7]. Описание этапов такого рода действий может быть получено лишь в результате функционального и аналитического моделирования. При этом функциональные модели рассматриваются как средство первичной формализации в интересах построения аналитических моделей оценки вероятностно-времен-ных характеристик процессов реализации каналов утечки и защиты информации от утечки.

Используемое в настоящее время методическое обеспечение оценки защищенности информации от утечки по техническим каналам, возникающим за счет ПЭМИ СЭ ОИ, не позволяет обеспечить адекватность математического представления исследуемых процессов на ОИ и как следствие в полной мере применить аппарат математического моделирования для решения задач оценки и повышения защищенности информации от утечки по каналам рассматриваемого типа [8].

В [7] предложен подход к формированию вербальных и функциональных моделей процессов реализации ТКУИ рассматриваемого типа в условиях динамики выполнения нарушителем соответствующих противоправных действий. Однако в этих моделях не учитываются возможности выполнения легитимными пользователями действий по реализации мер защиты информации от утечки в этих условиях. Случайный характер временных характеристик информационных процессов (ИПр), реализуемых легитимными пользователями, и процессов перехвата информации (ПрПИ), реализуемых нарушителем за счет ПЭМИ, обусловливает необходимость реализации легитимными пользователями соответствующих мер защиты.

В соответствии с действующим в настоящее время подходом к обеспечению защиты информации ИС предъявляются требования, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 [3].

В соответствии с этим нормативным документом на ОИ должна быть предусмотрена защита информации, представленной в виде информативных электрических сигналов и физических полей, т.е. ее защита от утечки по ТКУИ за счет ПЭМИ. Однако в базовом наборе мер защиты информации, используемом в качестве основы для выбора этих мер, для установленного класса защищенности ОИ предусмотрены меры организационно-режимного характера и не предусмотрены меры защиты информации, обрабатываемой техническими средствами от утечки по техническим каналам.

В методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» [9] указано, что защита информации от утечки по техническим каналам должна осуществляться в соответствии со специальными требованиями и рекомендациями по технической защите конфиденциальной информации [2], а также в соответствии с иными методическими документами ФСТЭК России по защите информации в государственных информационных системах от утечки по техническим каналам. При этом должны учитываться структурно-функциональные характеристики ОИ, режимы обработки информации на ОИ и в его отдельных элементах, а также иные характеристики ОИ, применяемые информационные технологии и особенности его функционирования.

Следует отметить, что в [2] лишь декларируются требования к защите конфиденциальной информации и приводятся некоторые рекомендации по их выполнению («как должно быть»), в основном с использованием мер организационно-режимного характера.

Вместе с тем в соответствии с современным подходом к защите информации меры защиты выбираются предварительно на этапе проектирования и разработки ОИ, а применяются эти меры на этапе эксплуатации без учета динамики реализации ТКУИ, возникающих за счет ПЭМИ СЭ ОИ. Это обусловлено использованием в качестве методического обеспечения такого выбора инструментально-расчетных методик для оценки защищенности информации от утечки по ТКУИ рассматриваемого типа. В качестве показателя для такой оценки в этих методиках используются измеренные значения отношения сигнал / шум и рассчитанные на основе этих измерений размеры контролируемой зоны (КЗ) вокруг объекта [10]. Как показано в [11], использование этих методик не позволяет достаточно точно оценить защищенность информации от утечки. При этом учитываются только энергетические характеристики информативного сигнала ПЭМИ и частично (в пределах КЗ) – характеристики среды его распространения и не учитываются характеристики других элементов описания ТКУИ – используемого разведывательного приемника, среды распространения перехватываемого сигнала ПЭМИ за пределами КЗ и тем более не учитываются возможности нарушителя по реализации различных вариантов стратегии применения технических средств разведки.

В соответствии с определением стратегии, приведенным в [12], перехват информации с использованием технических средств может осуществляться нарушителем [2]:

– из-за границы КЗ из близлежащих строений и транспортных средств;

– из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенных в том же здании, что и объект защиты;

– при посещении учреждения (предприятия) посторонними лицами;

– за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в ИС, как с помощью технических средств ИС, так и через информационные сети общего пользования.

Для перехвата информации могут использоваться разнообразные технические средства, как портативные возимые и носимые, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, так и стационарные, размещаемые в близлежащих строениях.

Нарушитель не имеет возможности воздействия на условия формирования ПЭМИ в пределах КЗ ОИ. Однако за пределами КЗ у него имеется множество вариантов выбора средств разведки в зависимости от условий их применения. При этом изменяются характеристики СЭ ТКУИ (среды распространения информативного сигнала, средств технической разведки). Эти изменения носят случайный характер [13, 14], и решение вопросов их учета в целях обеспечения защиты информации от утечки представляет достаточно сложную задачу.

Современное методическое обеспечение защиты информации от перехвата по техническим каналам, возникающим за счет ПЭМИ СЭ ОИ, не позволяет решить данную задачу. Это обусловлено особенностями функционирования ОИ, разнообразием номенклатуры и разнородностью радиоэлектронных устройств (РЭУ), используемых в составе ТС ОИ, а также неопределенностью относительно действий нарушителя по реализации процесса ПрПИ перехвата информации по ТКУИ, СЭ которых могут иметь различные характеристики [15–18].

СЭ ОИ взаимосвязаны через их параметры и характеристики. Вид и значения этих параметров и характеристик в существенной степени определяются формой представления информации. В зависимости от формы представления информации при реализации информационных процессов используются элементы структуры ОИ, обеспечивающие выполнение этих требований [16, 17].

Указанные взаимосвязи представлены на рис. 1 [18].

В обобщенном виде функционирование ОИ рассматриваемого типа может быть представлено в виде совокупности множеств и процессов:

$$\mathbf{\Phi}_{\text{ОИ}} = \{\mathbf{M}, \mathfrak{R}, \mathbf{Pr}, \text{ИПр}, \text{ПрПИ}, \text{ПрЗИ}\}, \qquad (1)$$

где $\mathbf{M} = \{\text{м}_i, i = 1, 2, \ldots I\}$ – множество массивов различного вида информации, формируемых источником информации (ИИ); $\mathfrak{R} = \{\rho_j, j = 1, 2, \ldots, J\}$ – множество РЭУ в структуре ОТСС (на рис. 1 РЭУ ρ_j в общем виде обозначены как СЭ e_j основного канала связи ОИ, используемого для реализации процесса ИПр передачи информации на ОИ); $\mathbf{Pr}=\{pr_k, k=1,2,...,K\}$ – множество мер, применяемых для реализации процесса защиты информации (ПрЗИ).

Реализация указанных информационных процессов осуществляется в условиях многофакторных взаимосвязей разнородных РЭУ СЭ ОТСС из (1).

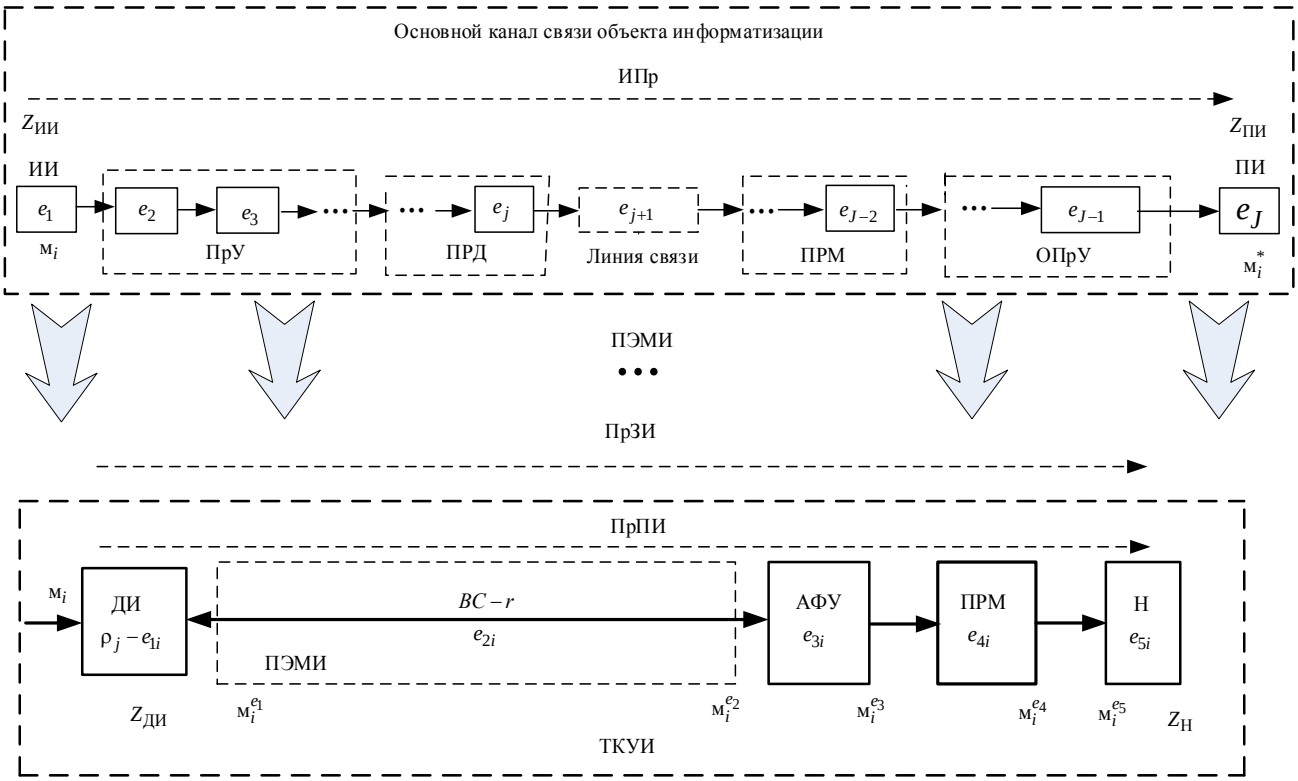


Рис. 1. Структурно-логическое представление процесса передачи информации на объекте информатизации и процесса ее перехвата за счет ПЭМИ радиоэлектронных устройств объекта

Так, ИПр информационный процесс может быть реализован при выборе в качестве СЭ ОИ РЭУ $\{\rho_j\}_i$ из множества $\Re$, использование которых обеспечит выполнение условия $Z_{\text{ПИ}} = Z_{\text{ПИ}}^{\text{тр}}$ для массива информации м$_i$:

$$\text{ИПр} = \left\{ \begin{matrix} \text{м}_i = \{\rho_j\}_i, \\ Z_{\text{ИИ}}, Z_{\text{ПИ}} \geq Z_{\text{ПИ}}^{\text{тр}}, \end{matrix} \right\} \quad (2)$$

где $Z_{\text{ИИ}}$ и $Z_{\text{ПИ}}$ – показатели ценности информации, характеризующие ее основные свойства для отправителя и получателя соответственно, $Z_{\text{ПИ}} = Z_{\text{ИИ}} \times K_0\{\rho_j\}_i$; $K_0\{\rho_j\}_i$ – коэффициент передачи выбранной траектории $\{\rho_j\}_i$ реализации ИПр; $Z_{\text{ПИ}}^{\text{тр}}$ – показатель ценности информации, удовлетворяющий требованиям получателя; $\hat{=}$ – знак соответствия.

Соответствие $\text{м}_i \hat{=} \{\rho_j\}_i$ означает выполнение условия [14]

$$V_{\text{м}_i} \leq C_{\{\rho_j\}_i}, \quad (3)$$

где $V_{\text{м}_i} = A_{\text{м}_i} \times \Delta f_{\text{м}_i} \times \Delta\tau_{\text{м}_i}$ – объем информационного сигнала массива м$_i$; $A_{\text{м}_i}, \Delta f_{\text{м}_i}, \Delta\tau_{\text{м}_i}$ – амплитуда, ширина спектра частот и продолжительность передачи информационного сигнала этого массива соответственно; $C_{\{\rho_j\}_i} = \mu_{\{\rho_j\}_i} \times \Delta F_{\{\rho_j\}_i} \times \Delta\tau_{\{\rho_j\}_i}$ – пропускная способность СЭ тракта передачи информации массива м$_i$; $\mu_{\{\rho_j\}_i}, \Delta F_{\{\rho_j\}_i}, \Delta\tau_{\{\rho_j\}_i}$ – чувствительность, полоса пропускания и время функционирования в заданном режиме РЭУ траектории реализации процесса ИПр передачи информации массива м$_i$.

Соответствие $Z_{\text{ПИ}} = Z_{\text{ПИ}}^{\text{тр}}$ означает выполнение условия [14]

$$V_{(\text{ПИ})_i} \geq V_{(\text{ПИ})_i}^{\text{тр}}, \quad (4)$$

где $V_{(\text{ПИ})_i}$ – объем информационного сигнала массива м$_i$, принимаемого получателем информации; $V_{(\text{ПИ})_i}^{\text{тр}}$ – объем информационного сигнала массива м$_i$, удовлетворяющий его требованиям.

Как показано в [16, 17], РЭУ из $\{\rho_j\}_i$ используются в качестве преобразующих, передающих, приемных и обратных преобразующих устройств (ПрУ, ПРД, ПРМ и ОПрУ соответственно). При этом из этих РЭУ формируется необходимая траектория преобразований, а процесс ИПр реализуется по пути $(e_1 \to e_2 \to \ldots \to e_J)$.

СЭ $e_1 - e_J$ в рамках траектории взаимосвязаны. Их взаимосвязи осуществляются путем согласования выходных характеристик предыдущего с входными характеристиками последующего СЭ в выбранной траектории [17]. Согласование обеспечивается в соответствии с условием (3). При этом в качестве выходных (сигнальных) характеристик рассматриваются амплитуда сигнала $A_{e_{j-1}}^c$, $j = 2, 3, \ldots, J$, $\Delta f_{e_{j-1}}^c$, ширина его спектра, а также промежуток времени $\Delta\tau_{e_{j-1}}^c$, в течение которого значения этих характеристик соответствуют требованиям к свойствам передаваемой информации. В качестве входных (сигнальных) характеристик рассматриваются $\mu_{e_j}^{lin}$ – чувствительность j-го СЭ к этим сигналам, его $\Delta F_{e_j}^{lin}$ – полоса пропускания и промежуток времени $\Delta\tau_{e_j}^{lin}$, в течение которого обеспечивается согласование. В соответствии с условиями согласования, описанными в [7], в обобщенном виде реализация ИПр может быть представлена в виде:

$$V_{e_1}^{\text{м}_i} \hat{=} C_{e_2}^{lin} \to V_{e_2}^{\text{м}_i} \hat{=} C_{e_3}^{lin} \to \ldots \to V_{e_{j-1}}^{\text{м}_i} \hat{=} C_{e_j}^{lin}. \quad (5)$$

В результате преобразований информационного сигнала на каждом из этапов $e_1 - e_j$ изменяются его параметры, определяющие основные свойства передаваемой информации, характеризующие ее ценность для обеспечиваемой деятельности.

Каждое РЭУ из подмножества $\{\rho_j\}_i$ может выступать в качестве источника ПЭМИ, как датчика информации в структуре ТКУИ, используемого нарушителем для реализации процесса ПрПИ перехвата информации массива м$_i$.

В соответствии с определением [4] ТКУИ может быть представлен в виде:

$$\text{ТКУИ} = \{\mathbf{M}, \mathfrak{R}_i, \mathbf{D}_j, Int_j\}, \quad (6)$$

где $\mathfrak{R}_i = \{\rho_j\}_i$ – подмножество РЭУ из $\mathfrak{R}$, которые могут быть использованы в качестве ДИ в структуре ТКУИ; $\mathbf{D}_j = \{d_{jm}, m = 1, 2, \ldots, M\}$ – множество направлений распространения ПЭМИ j-го РЭУ ОИ, используемых для реализации процесса ПрПИ перехвата информации.

$\mathbf{Int}_{ji} = \{int_{jiv}, v = 1, 2, \ldots, V\}$ – подмножество разведывательных радиоприемников (РРП) из их множества $\mathbf{Int} = \{int_v, v = 1, 2, \ldots, V\}$, которые могут быть использованы для приема ПЭМИ j-го РЭУ, модулированных информационным сигналом массива м$_i$.

Процесс ПрПИ перехвата информации за счет ПЭМИ этих РЭУ может быть реализован при выполнении условий

$$\text{ПрПИ} = \left\{ \begin{matrix} V_{\text{м}_i} \hat{=} V_{\rho_{ji}}^{\text{ПЭМИ}}, V_{\rho_{ji}}^{*\text{ПЭМИ}} \hat{=} int_{vji}, \\ Z_{\text{м}_i\text{Н}}^{*} \hat{=} Z_{\text{м}_i\text{Н}}^{*\text{тр}}, \end{matrix} \right\} \quad (7)$$

где $V_{\text{м}_i} \hat{=} V_{\rho_{ji}}^{\text{ПЭМИ}}$ – условие возможности использования j-го РЭУ ОТСС ОИ в качестве источника (датчика) ПЭМИ, модулированных информационным

сигналом массива $м_i$; $V_{\rho_{ji}}^{ПЭМИ}$ и $V_{\rho_{ji}}^{*ПЭМИ}$ – объемы сигналов ПЭМИ, модулированных информационным сигналом массива $м_i$, на выходе *j*-го РЭУ ОТСС ОИ и на входе *v*-го РРП, соответственно;

$$V_{\rho_{ji}}^{*ПЭМИ} = V_{\rho_{ji}}^{ПЭМИ} \times (1 - K_0(d_{jm}));$$

$K_0(d_{jm})$ – коэффициент ослабления ПЭМИ *j*-го РЭУ ОИ в *m*-м (*m* = 1, 2, …, *M*) направлении среды их распространения; $V_{\rho_{ji}}^{*ПЭМИ} \triangleq int_{jiv}$ – условие возможности использования *v*-го РРП для приема ПЭМИ этих РЭУ; $Z_{м_i Н}^{*} \triangleq Z_{м_i Н}^{*\,тр}$ – условие выполнения требований нарушителя к свойствам перехватываемой информации, $Z_{м_i Н}^{*}$ – показатель ценности перехваченной нарушителем информации массива $м_i$, характеризующий ее основные свойства; $Z_{м_i Н}^{*\,тр}$ – показатель ценности перехваченной информации, удовлетворяющий требованиям нарушителя.

Вербальная модель ТКУИ, используемого для реализации процесса ПрПИ перехвата информации в условиях отсутствия мер защиты, описана в [7]. Графическая иллюстрация этой модели по аналогии с [7] приведена на рис. 1.

В соответствии с описанием из всего множества $\mathfrak{R}$ РЭУ ОИ чувствительными к воздействию информационного сигнала массива $м_i$ могут быть лишь РЭУ из подмножества $\mathfrak{R}_i$ [19]. На выходе каждого РЭУ из $\{\rho_j\}_i$ (СЭ e_{1i} на рис. 1) формируется ПЭМИ в виде отклика на входное воздействие с характеристиками

$$V_{\rho_{ji}}^{ПЭМИ} = A_{\rho_{ji}}^{ПЭМИ} \times \Delta f_{\rho_{ji}}^{ПЭМИ} \times \Delta\tau_{\rho_{ji}}^{ПЭМИ}, \qquad (8)$$

где $A_{\rho_{ji}}^{ПЭМИ}, \Delta f_{\rho_{ji}}^{ПЭМИ}, \Delta\tau_{\rho_{ji}}^{ПЭМИ}$ – амплитуда, ширина спектра частот и промежуток времени, в течение которого СЭ $\{\rho_j\}_i$ может использоваться в качестве ДИ соответственно.

Как показано в [20], диаграмма направленности ПЭМИ может отличаться от круговой. Нарушитель в процессе реализации ПрПИ выбирает направление максимального уровня ПЭМИ, обеспечивающего минимальное значение коэффициента их ослабления $K_0(d_{jm})$. Для этих целей используется РРП с характеристиками, соответствующими характеристикам перехватываемого сигнала ПЭМИ $V_{\rho_{ji}}^{*ПЭМИ}$.

Таким образом, из множеств разнородных СЭ ТКУИ из (6) нарушитель формирует траекторию реализации ПрПИ с целью обеспечения согласования этих СЭ по аналогии с (5). В соответствии с условиями согласования, описанными в [7], в обобщенном виде реализация нарушителем ПрПИ может быть представлена в виде

$$V_{e_{1i}}^{\rho_i} \triangleq C_{e_{2i}}^{lin} \to V_{e_{2i}} \triangleq C_{e_{3i}}^{lin} \to V_{e_{3i}} \triangleq C_{e_{4i}}^{lin} \to V_{e_{4i}} \triangleq C_{e_{5i}}^{lin}. \quad (9)$$

Динамика реализации процессов ИПр и ПрПИ характеризуется их временными характеристиками.

Поскольку ТКУИ рассматриваемого типа реализуются с использованием РРП без воздействия на средства реализации ИПр, то защите от утечки подлежит только информация, передаваемая по основному каналу связи на ОИ. В связи с этим динамика реализации процесса ИПр характеризуется временными характеристиками, определяющими продолжительность передачи информации на ОИ, такими как начало, окончание и промежуток времени передачи самой информации. При этом учитывается время передачи $\Delta\tau_{м_i}$ при условии выполнения требований легитимных пользователей к свойствам передаваемой информации, характеризуемым амплитудой $A_{м_i}$ и шириной спектра $\Delta f_{м_i}$ сигнала как ее материального носителя на каждом из этапов преобразований [21]. Указанные характеристики носят случайный характер и отличаются для ОИ различного назначения.

Нарушитель при реализации процесса ПрПИ выполняет совокупность действий, связанных с обнаружением ПЭМИ [22], определением направления максимального уровня излучения, выбором РРП и настройкой режимов его работы с целью обеспечения требований к основным свойствам, характеризующим ценность перехватываемой информации. Эти действия направлены на выполнение условий (3) и (4) относительно ПЭМИ РЭУ ОИ на каждом этапе преобразований в процессе ПрПИ. Времена выполнения указанных действий носят случайный характер и зависят от множества различных факторов, описанных в [21]. В связи с этим далее при определении временных характеристик действий, составляющих содержание исследуемых процессов, будем учитывать средние значения этих времен ($\overline{\tau}$).

Общее описание мер защиты информации от утечки за счет ПЭМИ РЭУ ОИ

В соответствии с существующим методическим подходом защита информации на ОИ достигается проектно-архитектурными решениями, проведением организационных и технических мероприятий, а также выявлением портативных электронных устройств перехвата информации. Меры защиты информации от утечки за счет ПЭМИ РЭУ ОИ реализуются предварительно, и они не адаптированы к условиям динамики реализации нарушителем процесса ПрПИ. Следует отметить, что не всегда имеется возможность реализации проектно-архитектурных решений и указанных мероприятий в объеме, обеспечивающем требуемый уровень защищенности информации. Например, в условиях плотной городской застройки возникают трудности с выбором помещения, обеспечением необходимых размеров КЗ вокруг ОИ или с применением активных мер защиты информации, таких как пространственное зашумление СЭ объекта.

В этих условиях защита информации от утечки может быть обеспечена путем применения организационно-технических адаптивных мер защиты.

С целью выбора таких мер обратимся к структурно-логическому представлению основного и побочного каналов на рис. 1.

Выбор РЭУ ОИ $(\rho_j)_i$ для использования в качестве ДИ в структуре ТКУИ определяется их характеристиками, наиболее важными из которых являются [19]:

– чувствительность (отношение изменения выходного сигнала к изменению сигнала на его входе);

– разрешающая способность (точность преобразования);

– линейность (равномерность изменения выходного сигнала в зависимости от входного);

– инерционность или время отклика (время установления выходного сигнала в ответ на изменение входного);

– полоса частот (диапазон частот, в котором входное воздействие воспринимается преобразователем с допустимым уровнем отклика на выходе).

При этом амплитуда и спектр ПЭМИ на выходе ДИ зависят от амплитуды и спектра сигнала входного воздействия. В качестве мер защиты могут применяться технические решения по регулированию амплитуды сигнала и ограничению ширины его спектра в основном канале связи при условии обеспечения требований к свойствам информации, определяющим ее ценность для получателя. Эти технические решения могут быть реализованы предварительно на этапах проектирования и разработки ОИ. Однако если ограничение ширины спектра сигнала не влияет на динамику изменения спектральных характеристик ПЭМИ на выходе ДИ, то регулирование амплитуды сигнала $A_{\text{м}_i}$ позволит обеспечить соответствующее регулирование амплитуды ПЭМИ $A_{\rho_{ji}}^{\text{ПЭМИ}}$. При этом в качестве ограничения учитывается обеспечение заданных свойств передаваемой по основному каналу связи информации.

Регулирование амплитуды сигнала в основном канале может осуществляться как в автоматическом режиме, так и непосредственно перед реализацией процесса ИПр при настройке режима работы ТС ОИ.

Адаптационные методы повышения защищенности информации информационных систем известны [23]. Возможности их использования в рассматриваемых целях обусловлены избыточностью энергетики современных систем передачи информации при необходимости обеспечения требований легитимных пользователей к свойствам передаваемой информации, характеризующим ее ценность для обеспечиваемой деятельности.

Эффективность этих методов зависит от частоты передачи информационных сигналов на ОИ и соответственно от частоты ПЭМИ.

Так, в соответствии с действующими трехзонными расчетно-измерительными методиками для определения уровней напряжённости электрического (магнитного) поля используется рассчитанное значение коэффициента ослабления ПЭМИ $K_0(r)$:

$$E(r) = |_{r=R} = E(r)|_{r=d} \cdot K_0(r), \qquad (10)$$

$$H(r) = |_{r=R} = H(r)|_{r=d} \cdot K_0(r), \qquad (11)$$

где d – расстояние r до опорной (измерительной) точки в опасном направлении излучения.

Зависимости данного коэффициента от расстояния r для различных «зон» при типовом значении $d = 1$ м определяются по формулам [24]:

$K_0(r) \gg 1/r^3$ – для ближней зоны при $d < r \le L_б$, где $L_б$ – условная граница между ближней и промежуточной зонами; $K_0(r) \approx 1/r^2$ – для промежуточной зоны при $L_б < r \le L_д$, где $L_д$ – условная граница между промежуточной и дальней зонами; $K_0(r) \approx 1/r$ – для дальней зоны при $r \ge L_д$,

$$L_б = \lambda/2\pi, L_д = 6\lambda \text{ при } L_б \ge d. \qquad (12)$$

Из (12) видно, что с уменьшением длины волны ПЭМИ уменьшаются размеры соответствующих зон и соответственно изменяется вид зависимости коэффициента $K_0(r)$ от расстояния r.

В [11] приведена точная формула для коэффициента ослабления ПЭМИ $K_0(r)$ по электрическому и магнитному полю

$$K_{0E}(r) = K_{0H}(r) = \frac{d^3}{r^3}\sqrt{\frac{k^4r^4 - k^2r^2 + 1}{k^4d^4 - k^2d^2 + 1}}, \qquad (13)$$

где $k = 2\pi/\lambda$ – волновое число.

В (13) зависимость $K_0(r)$ от частоты излучения (волнового числа) представлена в явном виде.

Рассмотрим пример, приведенный в [21]. При передаче на ОИ речевой информации с использованием средств звукоусиления и колебаний электрического тока в аналоговом виде в качестве материального носителя этой информации существует опасность перехвата ПЭМИ этих средств уже в ближней зоне на расстоянии в несколько десятков метров.

Так, при коэффициенте усиления усилителя низкой частоты (УНЧ) на уровне 60 дБ и измеренном уровне ПЭМИ от него $E(r)|_{r=1\text{м}} \approx 100$ мВ/м на расстоянии 50 м от источника ПЭМИ $E(r)|_{r=50} \approx 0{,}8$мкВ/м, что выше уровня чувствительности большинства РРП, и перехват такого рода информации становится возможным.

Ограничение коэффициента усиления УНЧ до уровня 40 дБ и измеренного уровня ПЭМИ от него до $E(r)|_{r=1\text{м}} \approx 100$мВ/м на расстоянии 50 м от источника ПЭМИ $E(r)|_{r=50} \approx 0{,}8$мкВ/м, что ниже уровня чувствительности этих РРП. При этом с целью обеспечения условий приема нарушителю необходимо уменьшить расстояние r до источника ПЭМИ. При r=25 м $E(r)|_{r=25} \approx 0{,}6$мкВ/м. Для этих целей нарушителю потребуется дополнительное время $\bar{\tau}_{pl}^{ext}$ на выбор места применения РРП с точки зрения скрытности и $\bar{\tau}_{in}^{ext}$ на время сканирования частотного диапазона [7].

Уменьшение амплитуды ПЭМИ $A_{\rho_{ji}}^{\text{ПЭМИ}}$ может быть достигнуто также путем экранирования ТС ОИ. Однако это приводит к увеличению стоимости ТС ОИ.

Рассмотрим условия реализации нарушителем ПрПИ в соответствии со структурно-логическим представлением на рис. 1.

Будем считать, что нарушитель выполняет указанные выше действия на территории, прилегающей к КЗ ОИ. В связи с тем, что эти действия носят противоправный характер, легитимные пользователи могут применять меры защиты, направленные на их локализацию.

Поскольку указанные меры защиты направлены на локализацию противоправных действий нарушителя, выполняемых на прилегающей к КЗ ОИ территории, то временные характеристики этих мер рассмотрим относительно временных диаграмм реализации процессов ИПр и ПрПИ, приведенных в [7].

На рис. 2, *а* представлены временные диаграммы, иллюстрирующие повышение защищенности информации информационных систем от утечки за счет ПЭМИ РЭУ ОИ путем применения технических решений по ослаблению уровня ПЭМИ, а на рис. 2, *б* для сравнения приведены временные диаграммы процессов передачи информации на объекте информатизации и реализации ТКУИ при параллельном выполнении действий, обеспечивающих перехват информации, исследование которых проводилось в [7]. При этом по аналогии с [7] в течение времени $\overline{\tau}_{(1)}$ нарушителем выполняются действия, направленные на обеспечение возможности регистрации ПЭМИ РЭУ ОИ с использованием применяемого для этих целей РРП:

$$\left(A_{\text{ПЭМИ}}/P_{\text{ш}}\right) \geq \mu_{\text{РРП}}, \qquad (14)$$

где $A_{\text{ПЭМИ}}/P_{\text{ш}}$ – отношение амплитуды ПЭМИ к уровню шума на входе РРП; $\mu_{\text{РРП}}$ – чувствительность РРП.

В течение времени $\overline{\tau}_{(2)}$ нарушителем выполняются действия, направленные на выполнение его требований к свойствам перехватываемой информации в соответствии с условиями:

$$\Delta F_{\text{РРП}} \geq \Delta f_{\text{ПЭМИ}}, \qquad (15)$$

$$\Delta\tau_{\text{РРП}} \geq \Delta\tau_{\text{ПЭМИ}}, \qquad (16)$$

где $\Delta F_{\text{РРП}}$ и $\Delta f_{\text{ПЭМИ}}$ – полоса пропускания используемого в ТКУИ РРП и ширина спектра перехватываемого сигнала ПЭМИ соответственно; $\Delta\tau_{\text{РРП}}$ и $\Delta\tau_{\text{ПЭМИ}}$ – время функционирования РРП в заданном режиме и время, в течение которого ПЭМИ могут использоваться в качестве материального носителя перехватываемой информации.

С учетом последовательного выполнения действий, составляющих время $\overline{\tau}_{(1)}$, запишем:

$$\overline{\tau}_{(1)} = \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{dir} + \overline{\tau}_{cor}, \qquad (17)$$

где $\overline{\tau}_{pl}, \overline{\tau}_{in}, \overline{\tau}_{dir}, \overline{\tau}_{cor}$ – средние времена выполнения нарушителем противоправных действий, определенных в [7]; $\overline{\tau}_{ob}^{ext}, \overline{\tau}_{in}^{ext}$ – средние дополнительные времена выполнения действий по выбору места применения и сканирования частотного диапазона, обусловленные применением на ОИ технических решений по адаптивному регулированию уровня ПЭМИ.

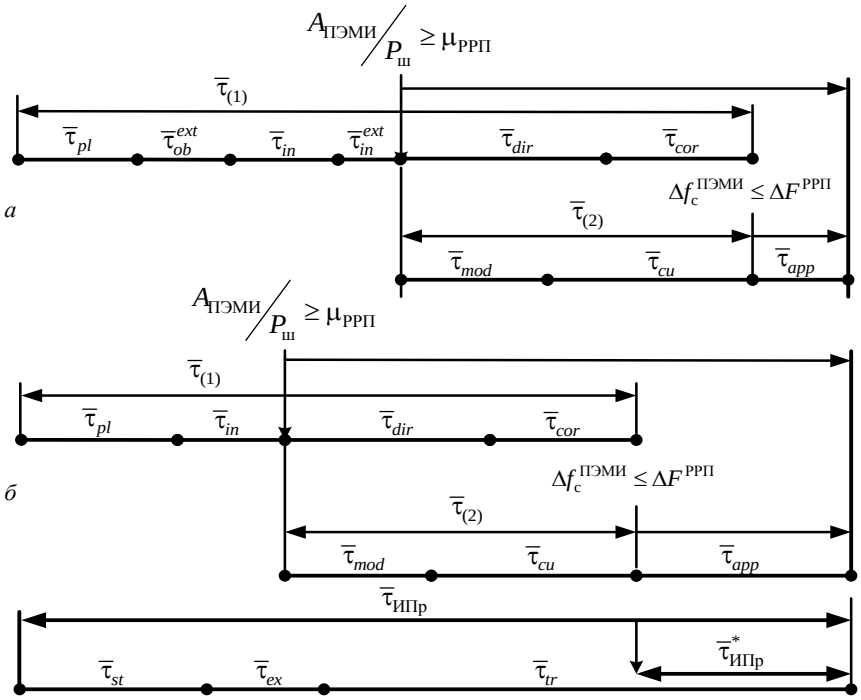


Рис. 2. Временные диаграммы повышения защищенности информации от утечки за счет ПЭМИ РЭУ ОИ путем применения технических решений по ослаблению уровня ПЭМИ при параллельном выполнении нарушителем действий, обеспечивающих реализацию процесса ПрПИ

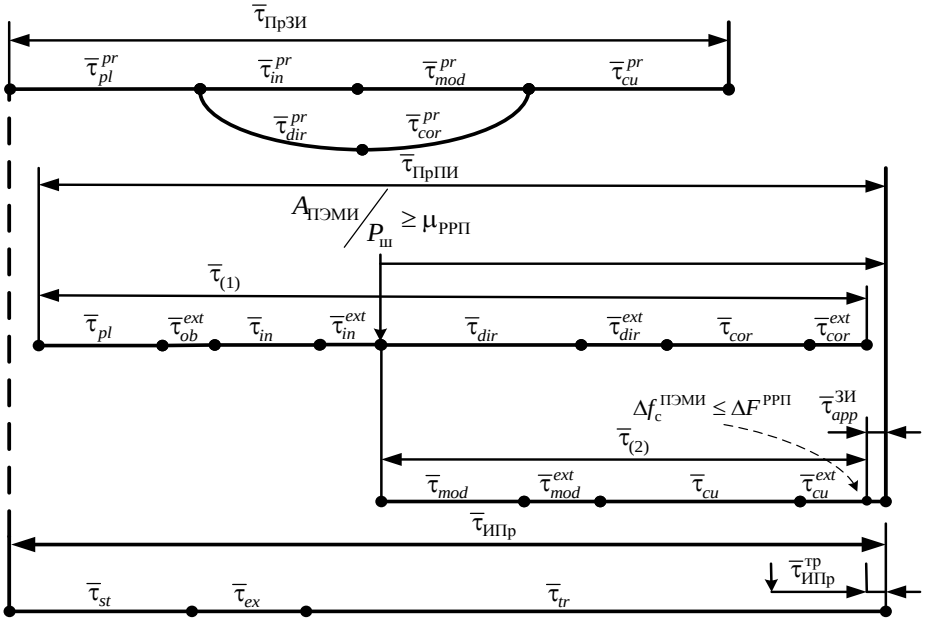


Рис. 3. Временные диаграммы адаптивных мер защиты по локализации действий нарушителя по реализации процесса перехвата информации за счет ПЭМИ радиоэлектронных устройств объекта информатизации

Содержание и времена выполнения нарушителем действий $\overline{\tau}_{\text{mod}}$ выбора режима работы РРП и $\overline{\tau}_{cu}$ настройки этого режима с учетом спектра сигнала ПЭМИ, составляющих время $\overline{\tau}_{(2)}$, а также среднее время применения РРП в режиме перехвата информации $\overline{\tau}_{app}$ и условия успешной реализации ПрПИ аналогичны приведенным в [7].

Из рис. 2 видно, что технические решения, направленные на реализацию адаптационных методов повышения защищенности информации информационных систем, позволяют в некоторой степени увеличить время $\overline{\tau}_{(1)}$ выполнения противоправных действий по реализации процесса ПрПИ и за счет этого соответственно несколько повысить защищенность этой информации. Однако следует отметить, что эффективность этих решений ограничена неопределенностью относительно большинства действий нарушителя на территории, прилегающей к КЗ ОИ.

На рис. 3 приведены временные диаграммы выполнения адаптивных мер защиты по локализации действий нарушителя, выполняемых им на различных этапах реализации процесса ПрПИ.

В качестве таких мер следует рассматривать меры организационно-технического характера, включающие совокупность действий, выполняемых легитимными пользователями на этапах подготовки информационной системы к передаче информации и непосредственно в процессе ее передачи как без использования, так и с использованием специальных технических средств. Указанные действия могут выполняться как в пределах КЗ ОИ, так и на прилегающей к этой зоне территории.

В пределах КЗ ОИ целью выполнения указанных действий является исключение возможности применения нарушителем для перехвата ПЭМИ РЭУ ОИ РРП путем контроля обстановки в соседних с этим объектом помещениях. Объективная сторона возможности такого контроля заключается в наличии демаскирующих признаков действий нарушителя, применяющего РРП.

Демаскирующие признаки определяются возможностью использования в этих условиях нарушителем носимых или портативных РРП с техническими характеристиками, не позволяющими осуществлять перехват слабых и широкополосных сигналов в реальном масштабе времени.

К основным мерам рассматриваемого типа могут быть отнесены видеонаблюдение (в том числе с использованием технических средств), патрулирование прилегающей к помещению ОИ территории, радиоконтроль электромагнитной обстановки.

Поскольку эти меры реализуются в пределах КЗ ОИ, то продолжительность их реализации может соответствовать продолжительности реализации процесса ИПр, а для выполнения соответствующих действий могут привлекаться сотрудники штатных подразделений обеспечения безопасности объекта. В этих условиях противоправные действия нарушителя носят оперативный характер и в данной статье не рассматриваются.

В связи с тем, что за пределами КЗ ОИ территория возможного применения РРП с целью реализации перехвата информации за счет ПЭМИ РЭУ ОИ может быть достаточно обширной, а расстояния до источника ПЭМИ достаточно большими (десятки и сотни метров), нарушитель может применять для реализации ТКУИ более сложные и совершенные РРП, возимого (в салонах специально оборудованных автомобилей) или стационарного (в зданиях посольств, иностранных представительств, сторонних организаций) типа. В этих условиях целью применения мер защиты является локализация противоправных действий нарушителя на различных этапах реализации процесса ПрПИ.

На рис. 3 представлены временные диаграммы выполнения действий по реализации процесса ПрЗИ защиты речевой информации от утечки за счет ПЭМИ РЭУ ОИ, оборудованного средствами связи и звукоусиления, в условиях реализации нарушителем действий по перехвату этой информации в соответствии с временными диаграммами, приведенными в [7].

Поскольку действия легитимных пользователей в рамках реализации адаптивных мер защиты информации направлены на локализацию действий нарушителя, по аналогии с [7] обозначим $\overline{\tau}_{pl}^{pr}$, $\overline{\tau}_{in}^{pr}$, $\overline{\tau}_{dir}^{pr}$, $\overline{\tau}_{cor}^{pr}$ – временные характеристики мер, направленных на локализацию действий нарушителя по обеспечению условия (14), включающие времена: выбора места применения РРП, с точки зрения скрытности; сканирования частотного диапазона с целью обнаружения ПЭМИ РЭУ ОИ; определения направления максимального уровня излучения (диаграммы направленности АФУ ДИ); корректирования места применения РРП (с учетом расстояния *r*), обеспечивающего выполнение условия (14); $\overline{\tau}_{mod}^{pr}$ и $\overline{\tau}_{cu}^{pr}$ – временные характеристики мер, направленных на локализацию действий нарушителя по обеспечению условия (15), включающие времена выбора режима работы РРП и настройки этого режима с учетом ширины спектра перехватываемого сигнала ПЭМИ.

Указанные действия по реализации мер защиты могут выполняться как последовательно, так и параллельно. Суммарное время их выполнения не превышает время реализации процесса ИПр на ОИ, а результатом является либо полное исключение возможности реализации нарушителем процесса ПрПИ, либо нарушение условий (7) и, в частности, нарушение условия обеспечения требований нарушителя к свойствам перехваченной информации $Z^{*}_{\text{м}_i\text{Н}} \triangleq Z^{*\ \text{тр}}_{\text{м}_i\text{Н}}$. На рис. 3 это нарушение иллюстрировано условием

$$\overline{\tau}_{app}^{\text{ЗИ}} < \overline{\tau}_{\text{ИПр}}^{\text{тр}}, \qquad (18)$$

где $\overline{\tau}_{\text{ИПр}}^{\text{тр}}$ – часть информационного процесса, перехват информации в которой удовлетворяет требованиям нарушителя.

В качестве адаптивных мер защиты информации будем рассматривать:

– оперативное видеонаблюдение за территорией, прилегающей к КЗ ОИ, с использованием технических средств (или без их использования) с целью своевременного обнаружения действий нарушителя по выбору места применения РРП ($\overline{\tau}_{pl}^{pr}$);

– патрулирование этой территории сотрудниками подразделений обеспечения безопасности объекта без применения и с применением портативных средств радиоконтроля с целью локализации действий нарушителя по выбору места применения РРП и обнаружения их ПЭМИ как демаскирующих признаков использования сканерных РРП ($\overline{\tau}_{pl}^{pr}$ и $\overline{\tau}_{in}^{pr}$);

– применение мобильных (возимых или носимых) маломощных генераторов электромагнитного шума или передающих устройств, имитирующих ПЭМИ РЭУ ОИ, с целью локализации действий нарушителя по определению направления максимального уровня излучения реальных ПЭМИ и корректированию места применения РРП (с учетом расстояния *r*) ($\overline{\tau}_{dir}^{pr}$ и $\overline{\tau}_{cor}^{pr}$);

– применение носимых маломощных передающих устройств, имитирующих ПЭМИ РЭУ ОИ, с целью локализации действий нарушителя по выбору режима работы применяемого им РРП и настройки этого режима $\overline{\tau}_{mod}^{pr}$ и $\overline{\tau}_{cu}^{pr}$ и др.

Применение перечисленных мер направлено на обеспечение выполнения условия (18) за счет дополнительных временных затрат на выполнение нарушителем соответствующих действий:

$$\overline{\tau}_{ob}^{ext},\ \overline{\tau}_{in}^{ext},\ \overline{\tau}_{dir}^{ext},\ \overline{\tau}_{cor}^{ext},\ \overline{\tau}_{mod}^{ext}\ \text{и}\ \overline{\tau}_{cu}^{ext}.$$

В соответствии с рис. 3 в качестве времени реализации процесса ПрЗИ следует рассматривать:

$$\overline{\tau}_{\text{ПрЗИ}} = \max\begin{cases} \overline{\tau}_{pl}^{pr} + \overline{\tau}_{in}^{pr} + \overline{\tau}_{\text{mod}}^{pr} + \overline{\tau}_{cu}^{pr}, \\ \overline{\tau}_{pl}^{pr} + \overline{\tau}_{dir}^{pr} + \overline{\tau}_{cor}^{pr} + \overline{\tau}_{cu}^{pr}. \end{cases} \qquad (19)$$

В связи с тем, что эти меры могут выполняться как последовательно, так и параллельно, то их выполнение целесообразно корректировать по времени в соответствии с действиями нарушителя, на локализацию которых они направлены.

В этих условиях защита информации от утечки за счет ПЭМИ РЭУ ОИ будет обеспечена при выполнении условия (18). Неформально это означает, что реализация адаптивных мер защиты информации направлена на обеспечение условий, при которых непосредственный перехват нарушителем этой информации (в течение времени $\overline{\tau}_{app}^{\text{ЗИ}}$) может быть обеспечен только тогда, когда свойства информации, содержащейся в части перехваченного информационного процесса, не будут удовлетворять его требованиям $\overline{\tau}_{\text{ИПр}}^{\text{тр}}$.

Значения временных характеристик действий по реализации указанных мер защиты информации случайны. В связи с этим при определении временных характеристик исследуемых процессов будем учитывать их средние значения, которые могут быть определены либо экспертным путем, либо с использованием сведений о характеристиках ТС, используемых для их выполнения.

В рассмотренной вербальной модели процесса защиты информации от утечки за счет ПЭМИ РЭУ ОИ могут быть учтены и другие традиционные меры, а также рассмотренные в данной статье технические решения.

В соответствии с временными диаграммами, приведенными на рис. 3, без изменения оставим среднее время реализации информационного процесса $\overline{\tau}_{\text{ИПр}} \approx 35$ мин.

В табл. 1 приведены примерные значения временных характеристик указанных мер защиты информации, а также дополнительные времена выполнения нарушителем действий по реализации ПрПИ

для ОИ, исследование характеристик которого проводилось в [7].

Среднее время реализации процесса ПрПИ для варианта, соответствующего параллельному выполнению нарушителем действий, в соответствии с временными диаграммами, приведенными на рис. 2, определим с учетом дополнительных времен, обусловленных применением на ОИ адаптивных мер защиты в соответствии с условием

$$\overline{\tau}_{\text{ПрПИ}} = \max\begin{cases} \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{dir} + \overline{\tau}_{dir}^{ext}; \\ \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{\text{mod}} + \overline{\tau}_{\text{mod}}^{ext}. \end{cases} \quad (20)$$

При этом с учетом [7] и данных табл. 1 получим $\overline{\tau}_{\text{ПрПИ}} = \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{dir} + \overline{\tau}_{cor} \approx 42$ мин.

Очевидно, что в этих условиях перехват информации нарушителем становится нереализованным $\overline{\tau}_{\text{ИПр}} < \overline{\tau}_{\text{ПрПИ}}$ и ($\overline{\tau}_{app} = 0$).

Таблица 1

Временные характеристики действий, выполняемых при реализации процессов ПрЗИ и ПрПИ

№ п/п	Название характеристики и ее обозначение	Способ определения	Минимальное значение, мин	Максимальное значение, мин	Среднее значение, мин
1	Время оперативного видеонаблюдения за территорией, прилегающей к КЗ ОИ, без использования ТС – τ_{pl}^{pr}	Эксперт	4	6	5
2	Время патрулирования этой территории без применения средств радиоконтроля – τ_{pl}^{pr}	Эксперт	5	7	6
3	Дополнительное время выбора нарушителем места применения РРП в условиях адаптационных мер защиты информации на ОИ – τ_{ob}^{ext}	Эксперт	2	6	4
4	Дополнительное время выбора нарушителем места применения РРП – τ_{pl}^{ext}	Эксперт	5	7	6
5	Время патрулирования этой территории с применением средств радиоконтроля – τ_{m}^{pr}	Эксперт. Характеристики РРП	4	6	5
6	Дополнительное время работы РРП в режиме сканирования по частоте в связи с применением адаптационных мер защиты информации на ОИ – τ_{in}^{ext}	Эксперт	3	5	4
7	Дополнительное время работы РРП в режиме сканирования по частоте – τ_{in}^{ext}	Эксперт. Характеристики РРП	4	6	5
8	Время видеонаблюдения с последующим применением мобильных генераторов шума – τ_{dir}^{pr}	Регламент реализации ИПр	5	10	7,5
9	Дополнительное время определения нарушителем направления максимального уровня излучения ПЭМИ – τ_{dir}^{ext}	Регламент реализации ИПр	5	10	7,5
10	Время видеонаблюдения с последующим применением мобильных устройств имитации ПЭМИ – τ_{cor}^{pr}	Регламент реализации ИПр	5	10	7,5
11	Дополнительное время корректирования нарушителем места применения РРП – τ_{cor}^{ext}	Регламент реализации ИПр	5	10	7,5
12	Время применения носимых устройств, имитирующих ПЭМИ РЭУ ОИ, – τ_{mod}^{pr}	Характеристики устройств, имитирующих ПЭМИ	8	12	10
13	Дополнительное время выбора нарушителем режима работы РРП для перехвата реальных ПЭМИ – τ_{mod}^{ext}	Характеристики РРП	1	2	1,5
14	Время применения носимых устройств, имитирующих ПЭМИ РЭУ ОИ, модулированных тестовым информационным сигналом – τ_{cu}^{pr}	Характеристики устройств, имитирующих ПЭМИ	8	12	10
15	Дополнительное время настройки РРП в выбранном режиме – τ_{cu}^{ext}	Характеристики РРП	2	3	2,5
16	Время реализации перехвата информации в условиях мер защиты – $\tau_{app}^{\text{ЗИ}}$	Эксперт	1	2	1,5
17	Часть информационного процесса, перехват информации в которой удовлетворяет требованиям нарушителя, – $\tau_{\text{ИПр}}^{\text{тр}}$	Эксперт	4	6	5

Рассмотрим применение мер защиты в соответствии с временными диаграммами, приведенными на рис. 3.

При условии согласованного выполнения действий по реализации различных мер защиты информации в (19) среднее время реализации процесса ПрЗИ защиты информации составит

$$\overline{\tau}_{\text{ПрЗИ}} = \max\begin{cases} 5+5+10+10 \\ 5+7{,}5+7{,}5+10 \end{cases} \approx 30 \text{ мин.}$$

При этом среднее время реализации нарушителем процесса ПрПИ составит:

$$\overline{\tau}_{\text{ПрПИ}} = \max\begin{cases} \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{dir}^{ext} + \overline{\tau}_{cor} + \overline{\tau}_{cor}^{ext} \approx 56 \text{ мин,} \\ \overline{\tau}_{pl} + \overline{\tau}_{ob}^{ext} + \overline{\tau}_{in} + \overline{\tau}_{in}^{ext} + \overline{\tau}_{mod} + \overline{\tau}_{mod}^{ext} + \overline{\tau}_{cu} + \overline{\tau}_{cu}^{ext} \approx 51 \text{ мин,} \end{cases}$$

т.е. $\overline{\tau}_{\text{ПрПИ}} \approx 56$ мин.

Такое время реализации нарушителем процесса ПрПИ также не удовлетворяет его требованиям, так как заведомо не выполняется условие (18).

Особенности реализации процессов, временные диаграммы которых приведены на рис. 2 и 3, обусловлены следующими обстоятельствами:

– исследуемые процессы могут реализовываться параллельно и независимо один от другого;

– значения времен выполнения различных действий при их реализации случайны;

– при реализации каждого процесса составляющие его действия могут выполняться как последовательно, так и параллельно;

– результатом выполнения действий является обеспечение (или необеспечение) некоторых условий (например, (14)–(16), (18));

– для различных ОИ как состав, так и последовательность выполняемых действий отличаются.

Приведенные временные диаграммы и описания исследуемых процессов дают лишь общее представление об условиях их реализации. Однако они могут послужить основой для разработки функциональных и аналитических моделей в интересах оценки защищенности информации от утечки за счет ПЭМИ РЭУ на ОИ. При этом для различных ОИ соответствующие функциональные и аналитические модели также будут отличаться.

Функциональные модели защиты информации от утечки за счет побочных электромагнитных излучений радиоэлектронных устройств объектов информатизации

Для оценки защищенности информации от утечки за счет ПЭМИ РЭУ для конкретного ОИ в условиях отсутствия и применения мер защиты с учетом временного фактора необходимо определить времена выполнения действий, составляющих процессы, представленные на рис. 2 и 3, и последовательности их выполнения. Такие исследования ранее не проводились, а соответствующие модели не разрабатывались. Функциональные модели процессов защиты информации от утечки за счет ПЭМИ РЭУ ОИ также не разрабатывались.

В данной работе предложен подход к разработке таких моделей, по аналогии с [7] основанный на стратифицированном представлении исследуемых процессов, с учетом особенностей их реализации на различных уровнях (этапах) и наличия связей между ними, в соответствии с условиями (14)–(16) и (18) [25] (рис. 4).

В соответствии с таким представлением каждый из исследуемых процессов (ИПр, ПрПИ, ПрЗИ) реализуется в несколько этапов (страт). Каждая из страт представляет собой совокупность различных действий, выполняемых легитимными пользователями или нарушителем. Количество страт для различных процессов может отличаться. При этом действия на первой и конечной стратах выполняются при реализации всех процессов. Действия на некоторых промежуточных стратах для различных процессов в зависимости от условий их реализации могут не выполняться, и соответствующая страта пропускается. В этих условиях обеспечивается возможность представления взаимосвязей между действиями, выполняемыми не только на разных стратах, но и для разнородных параллельно реализуемых процессов, что позволяет в соответствии со сформированным в данной работе вербальным описанием их реализации по аналогии с [7, 26, 27] сформировать совокупность таких действий, выполняемых как параллельно, так и последовательно, для различных вариантов обеспечения защиты информации от утечки за счет ПЭМИ РЭУ ОИ. С учетом указанных взаимосвязей при выполнении действий на всех стратах описания моделируемых процессов создаются условия для формирования их функциональных моделей.

В качестве примера рассмотрим варианты реализации процессов ИПр, ПрПИ и ПрЗИ, представленные на рис. 3, с учетом исследований, проведенных в [7].

Первая страта функционального описания исследуемых процессов представляет собой совокупность действий, характеризующих настройку ТС ОИ в заданном режиме (время $\overline{\tau}_{st}$ в процессе ИПр), выбор нарушителем места применения РРП (время $\overline{\tau}_{pl}$ в процессе ПрПИ) и применение легитимными пользователями мер по оперативному наблюдению за территорией, прилегающей к КЗ ОИ и / или патрулирование этой территории без применения ТС или с применением средств радиоконтроля (время $\overline{\tau}_{pl}^{pr}$ в процессе ПрЗИ). Поскольку по окончании настройки ТС ОИ в заданном режиме возможно формирование ПЭМИ их РЭУ, и нарушитель имеет возможность выполнять соответствующие действия по реализации ПрПИ в то время, когда процесс непосредственной передачи информации еще не начинался, то на второй страте могут отсутствовать действия, связанные с реализацией процесса ИПр.

При этом вторая страта включает совокупность действий, связанных с корректированием нарушителем места применения РРП (дополнительное время $\overline{\tau}_{ob}^{ext}$), при условии применения легитимными пользователями мер защиты, выполненных на первой страте (время $\overline{\tau}_{pl}^{pr}$).

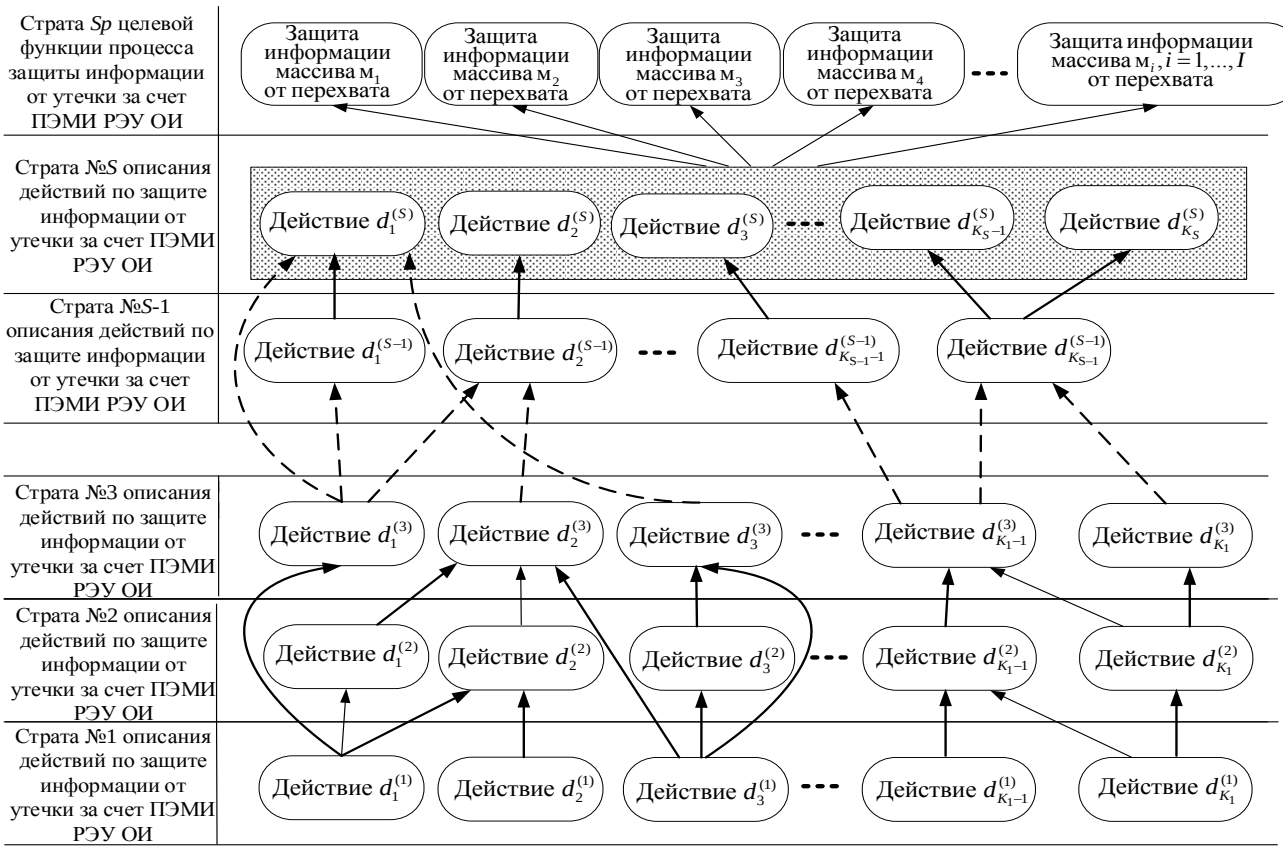


Рис. 4. Иллюстрация стратифицированного описания процесса защиты информации от утечки за счет побочных электромагнитных излучений радиоэлектронных устройств объекта информатизации

Страта 3 содержит действия по ожиданию передачи информации в процессе ИПр (время $\overline{\tau}_{ex}$), по сканированию нарушителем частотного диапазона с использованием РРП ($\overline{\tau}_{in}$), по применению легитимными пользователями средств радиоконтроля для обнаружения демаскирующих признаков работы РРП в режиме сканирования частотного диапазона (время $\overline{\tau}_{in}^{pr}$).

На последующих промежуточных стратах функционального описания исследуемых процессов выполняются в тесной взаимосвязи действия по реализации процессов ПрПИ и ПрЗИ нарушителем и легитимными пользователями соответственно.

Указанные действия характеризуются временными характеристиками, приведенными в табл. 1. При этом дополнительные времена выполнения нарушителем ряда действий обусловлены применением легитимными пользователями мер организационно-технического характера, направленных на их локализацию. В табл. 1 эти обстоятельства обозначены соответствием нижних и отличием верхних индексов в обозначениях времен, характеризующих соответствующие действия.

Так, оперативное видеонаблюдение за территорией, прилегающей к КЗ ОИ, выполняемое легитимными пользователями без использования ТС и характеризуемое временем $\overline{\tau}_{pl}^{pr}$, вынуждает нарушителя к выбору места применения РРП, обеспечивающего скрытность, что, в свою очередь, приводит к необходимости увеличения времени выполнения этого действия – $\overline{\tau}_{ob}^{ext}$. Патрулирование этой территории с применением средств радиоконтроля, характеризуемое временем $\overline{\tau}_{in}^{pr}$, обусловливает увеличение времени выполнения нарушителем действий по применению РРП в режиме сканирования частотного диапазона с целью обнаружения ПЭМИ – $\overline{\tau}_{in}^{ext}$. Оперативное видеонаблюдение, осуществляемое из автотранспорта, с последующим применением мобильных генераторов шума (время $\overline{\tau}_{dir}^{pr}$) приводит к увеличению времени выполнения нарушителем действий по определению направления максимального уровня излучения ПЭМИ ($\overline{\tau}_{dir}^{ext}$). Аналогичное обоснование имеют и другие последующие действия легитимных пользователей и нарушителя, временные характеристики которых приведены в табл. 1.

При этом действия легитимных пользователей могут либо опережать соответствующие действия нарушителя, либо выполняться с ними параллельно.

Совокупности указанных действий определяют взаимосвязи реализации процессов передачи информации на ОИ, ее перехвата за счет ПЭМИ РЭУ этого объекта и защиты от утечки за счет выполнения адаптивных мер защиты.

В качестве примеров рассмотрим некоторые из возможных вариантов представления совокупностей

действий, выполняемых при реализации процесса защиты информации, предаваемой на ОИ в условиях адаптации к угрозам утечки этой информации за счет ПЭМИ РЭУ этого объекта, в соответствии с рис. 4.

Целевая функция $d_2^{(Sp)}$ является результатом выполнения совокупности действий:

$$\left(d_1^{(3)} \,\&\, d_2^{(3)}\right) \to d_2^{(S-1)} \to d_2^{(S)} \to d_2^{(Sp)},$$

где действие $d_1^{(3)}$ выполняется после $d_1^{(1)}$: $d_1^{(1)} \to d_1^{(3)}$; действие $d_2^{(3)}$ – результат выполнения совокупности действий:

$$\left(\left(\left(d_1^{(1)} \to d_1^{(2)}\right) \& \left(\left(d_1^{(1)} \to d_2^{(1)}\right) \to d_2^{(2)}\right) \& d_3^{(1)}\right)\right) \to d_2^{(3)}.$$

Целевая функция $d_{м_i}^{(Sp)}$ является результатом выполнения совокупности действий:

$$\left(\left(d_{K_1-1}^{(3)} \,\&\, d_{K_1}^{(3)}\right) \to d_{K_{S-1}}^{(S-1)} \to d_{K_S}^{(S)} \to d_{м_i}^{(Sp)}\right),$$

где действия $d_{K_1-1}^{(3)}$ и $d_{K_1}^{(3)}$, в свою очередь, представляются в виде совокупностей действий:

$$\left(\left(\left(d_{K_1-1}^{(1)} \,\&\, d_{K_1}^{(1)}\right) \to d_{K_1-1}^{(2)}\right) \& \left(d_{K_1}^{(1)} \to d_{K_1}^{(2)}\right)\right) \to d_{K_1-1}^{(3)};$$

$\left(d_{K_1}^{(1)} \to d_{K_1}^{(2)}\right) \to d_{K_1}^{(3)}$, соответственно.

Приведенные совокупности действий при определенных условиях соответствуют иллюстрации параллельной реализации информационных процессов ПрЗИ, ПрПИ и ИПр, представленной на рис. 3.

Последовательно-параллельный характер выполнения совокупностей действий, характеризующих реализацию этих процессов, усложняет оценку общих времен их реализации. В соответствии с описаниями, приведенными выше, это усложняет оценку защищенности информации от утечки за счет ПЭМИ РЭУ ОИ как оценку соотношений этих времен с учетом условия (18).

В интересах такой оценки в условиях параллельной реализации рассматриваемых процессов для каждого из них необходимо определить композиции возможных совокупностей действий, выполненных на предыдущих стратах описания, и направленных на создание условий для их реализации.

При этом формально функциональная модель параллельной реализации процессов ПрЗИ, ПрПИ и ИПр с учетом [7] может быть представлена как совокупность множеств

$$\Phi_{\Pi} = \left\{ \begin{array}{l} \mathbf{D}_u^{\mathrm{I}}, \mathbf{M}(\mathbf{D}_u^{\mathrm{I}}), Y(\mathbf{D}_u^{\mathrm{I}}), u^{\mathrm{I}} = \overline{1, U^{\mathrm{I}}}; \\ \mathbf{D}_u^{\mathrm{II}}, \mathbf{M}(\mathbf{D}_u^{\mathrm{II}}), Y(\mathbf{D}_u^{\mathrm{II}}), u^{\mathrm{II}} = \overline{1, U^{\mathrm{II}}}; \\ \mathbf{D}_u^{\mathrm{III}}, \mathbf{M}(\mathbf{D}_u^{\mathrm{III}}), Y(\mathbf{D}_u^{\mathrm{III}}), u^{\mathrm{III}} = \overline{1, U^{\mathrm{III}}}, \end{array} \right\} \quad (21)$$

где $\mathbf{D}_u^{\mathrm{I}}$ – множество действий $d_u^{(k^{\mathrm{I}})} \in \mathbf{D}_u^{\mathrm{I}}$, $k^{\mathrm{I}} = \overline{1, K^{\mathrm{I}}}$, выполняемых для реализации u^{I}-го варианта процесса ПрЗИ, K^{I} – мощность множества $\mathbf{D}_u^{\mathrm{I}}$; $\mathbf{D}_u^{\mathrm{II}}$ – множество действий $d_u^{(k^{\mathrm{II}})} \in \mathbf{D}_u^{\mathrm{II}}, k^{\mathrm{II}} = \overline{1, K^{\mathrm{II}}}$, выполняемых для реализации u^{II}-го варианта ПрПИ; K^{II} – мощность множества $\mathbf{D}_u^{\mathrm{II}}$; $\mathbf{D}_u^{\mathrm{III}}$ – множество действий $d_u^{(k^{\mathrm{III}})} \in \mathbf{D}_u^{\mathrm{III}}, k^{\mathrm{III}} = \overline{1, K^{\mathrm{III}}}$, выполняемых для реализации u^{III}-го варианта ИПр, K^{III} – мощность множества D_u^{III}; $\mathbf{M}(D_u^{\mathrm{I}})$, $\mathbf{M}(D_u^{\mathrm{II}})$ и $\mathbf{M}(D_u^{\mathrm{III}})$ – матрицы взаимосвязей действий $d_u^{(k^{\mathrm{I}})}, d_u^{(k^{\mathrm{II}})}$ и $d_u^{(k^{\mathrm{III}})}$ соответственно, в порядке их выполнения; $Y(\mathbf{D}_u^{\mathrm{I}}), Y(\mathbf{D}_u^{\mathrm{II}})$ и $Y(\mathbf{D}_u^{\mathrm{III}})$ – совокупности условий для выполнения действий из их множеств, при которых реализация варианта соответствующего процесса возможна.

Несмотря на параллельность и независимость реализации рассматриваемых процессов, они взаимосвязаны через их характеристики. Так, реализация процесса ПрПИ становится невозможной в условиях, когда информация на ОИ не передается. Время выполнения ряда действий в процессе ПрПИ увеличивается в условиях выполнения определенных действий процесса ПрЗИ.

С учетом указанных взаимосвязей и представления (21) могут быть разработаны функциональные модели параллельно реализуемых процессов ПрПИ перехвата информации за счет ПЭМИ РЭУ ОИ, информационного процесса ИПр и процесса ПрЗИ защиты этой информации. Эти модели должны включать как совокупности выполняемых нарушителем действий, связанных с согласованием разнородных характеристик сигналов ПЭМИ с соответствующими характеристиками РРП в ТКУИ, так и действий, выполняемых легитимными пользователями в интересах нарушения условий согласования за счет адаптивных мер защиты информации. При разработке таких моделей следует учитывать взаимосвязи этих действий, условия их выполнения, а также примерные оценки времени выполнения.

В соответствии с указанным подходом на основе функциональных моделей реализации процесса ПрПИ перехвата речевой информации, циркулирующей в выделенном помещении, оборудованном средствами звукоусиления, разработанных в [7], на рис. 5 приведен вариант представления таких моделей с учетом выполнения легитимными пользователями рассмотренных выше адаптивных мер защиты этой информации от перехвата, соответствующий параллельному выполнению нарушителем действий по реализации процесса ПрПИ.

Обозначения и описания действий, выполняемых в ходе реализации моделируемых процессов, соответствуют данным, приведенным в табл. 1.

В обозначениях выполняемых действий верхние индексы соответствуют последовательности их выполнения в рамках соответствующего процесса, первая цифра нижнего индекса обозначает тип моделируемого процесса, вторая цифра соответствует виду защищаемой информации (например, массива $м_2$).

В табл. 2 приведены описания этих действий с учетом последовательностей их выполнения и взаимосвязей моделируемых процессов.

В табл. 2 средние времена выполнения действий указаны на основании экспертных оценок и известных характеристик используемых РРП.

В соответствии с моделью, приведенной на рис. 5 и с учетом данных табл. 2 при параллельном выполнении нарушителем некоторых действий, направленных на обеспечение условий (14) и (15), в соответствии с функциональной схемой время реализации процесса ПрПИ определяется по аналогии с условием (20).

$$\overline{\tau}_{\text{ПрПИ}} \approx \max \begin{cases} \tau\left(d_{2.2}^{(1)}\right)+\tau\left(d_{2.2}^{(2)}\right)+\tau\left(d_{2.2}^{(3)}\right)+\tau\left(d_{2.2}^{(4)}\right)+ \\ +\tau\left(d_{2.2}^{(5)}\right)+\tau\left(d_{2.2}^{(6)}\right)+\tau\left(d_{2.2}^{(7)}\right)+\tau\left(d_{2.2}^{(8)}\right); \\ \tau\left(d_{2.2}^{(1)}\right)+\tau\left(d_{2.2}^{(2)}\right)+\tau\left(d_{2.2}^{(3)}\right)+\tau\left(d_{2.2}^{(4)}\right)+ \\ +\tau\left(d_{2.2}^{(9)}\right)+\tau\left(d_{2.2}^{(10)}\right)+\tau\left(d_{2.2}^{(11)}\right)+\tau\left(d_{2.2}^{(12)}\right). \end{cases}$$

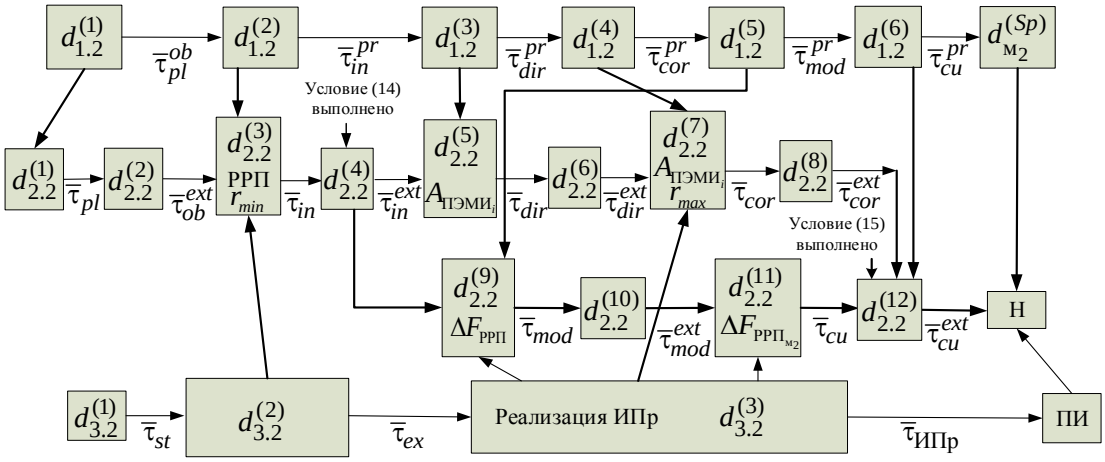
Таблица 2

Обозначения и содержание действий, выполняемых при реализации процесса перехвата речевой информации, циркулирующей в выделенном помещении, оборудованном средствами звукоусиления и связи

Название процесса	Содержание и обозначение среднего времени выполняемых действий при реализации процессов ПрЗИ, ПрПИ, ИПр	Обозначение действий	Среднее время выполнения действий, мин
1	2	3	4
Вариант № 1			
Реализация процессов защиты речевой информации, циркулирующей в выделенном помещении, оборудованном средствами звукоусиления и связи перехвата, от перехвата за счет ПЭМИ РЭУ ОИ	Оперативное видеонаблюдение легитимных пользователей за территорией, прилегающей к КЗ ОИ, без использования ТС – $\overline{\tau}_{pl}^{ob}$	$d_{1.2}^{(1)}$	5
	Нарушитель выбирает место применения РРП ($r = r_{\min}$), при котором обеспечиваются условия скрытности, – $\overline{\tau}_{pl}$	$d_{2.2}^{(1)}$	10
	Настройка ТС звукоусиления для передачи речевой информации на ОИ – $\overline{\tau}_{st}$	$d_{3.2}^{(1)}$	15
	Патрулирование территории, прилегающей к КЗ ОИ, с применением средств радиоконтроля – $\overline{\tau}_{in}^{pr}$	$d_{1.2}^{(2)}$	5
	Выбор нарушителем места применения РРП в условиях оперативного видеонаблюдения легитимных пользователей за территорией, прилегающей к КЗ ОИ – $\overline{\tau}_{ob}^{ext}$	$d_{2.2}^{(2)}$	4
	Ожидание передачи речевой информации на ОИ – $\overline{\tau}_{ex}$	$d_{3.2}^{(2)}$	10
	Применение нарушителем РРП в режиме сканирования частотного диапазона без применения адаптационных мер защиты информации на ОИ при выполнении условия (14) – $\overline{\tau}_{in}$	$d_{2.2}^{(3)}$	4
	Применение нарушителем РРП в режиме сканирования частотного диапазона в условиях применения адаптационных мер защиты информации на ОИ при выполнении условия (14) – $\overline{\tau}_{in}^{ext}$	$d_{2.2}^{(4)}$	4
	Видеонаблюдение с последующим применением мобильных генераторов шума – $\overline{\tau}_{dir}^{pr}$	$d_{1.2}^{(3)}$	7,5
	Реализация информационного процесса ИПр – $\overline{\tau}_{\text{ИПр}}$	$d_{3.2}^{(3)}$	35
	Определения нарушителем направления максимального уровня излучения ПЭМИ без применения адаптационных мер защиты информации на ОИ – $\overline{\tau}_{dir}$	$d_{2.2}^{(5)}$	6
	Определения нарушителем направления максимального уровня излучения ПЭМИ в условиях применения адаптационных мер защиты информации на ОИ – $\overline{\tau}_{dir}^{ext}$	$d_{2.2}^{(6)}$	7,5
	Видеонаблюдение с последующим применением мобильных устройств имитации ПЭМИ – $\overline{\tau}_{cor}^{pr}$	$d_{1.2}^{(4)}$	7,5
	Корректирование нарушителем места применения РРП без применения адаптационных мер защиты информации на ОИ – $\overline{\tau}_{cor}$	$d_{2.2}^{(7)}$	10
	Корректирование нарушителем места применения РРП в условиях применения адаптационных мер защиты информации на ОИ – $\overline{\tau}_{cor}^{ext}$	$d_{2.2}^{(8)}$	7,5
	Применение мобильных устройств, имитирующих ПЭМИ РЭУ ОИ, – $\overline{\tau}_{\text{mod}}^{pr}$	$d_{1.2}^{(5)}$	10

Окончание табл. 2

1	2	3	4
	Выбор нарушителем режима работы РРП для перехвата реальных ПЭМИ без применения мер защиты – $\overline{\tau}_{mod}$	$d_{2.2}^{(9)}$	4
	Выбор нарушителем режима работы РРП для перехвата реальных ПЭМИ в условиях применения мер защиты – $\overline{\tau}_{\text{mod}}^{ext}$	$d_{2.2}^{(10)}$	5
	Применение носимых устройств, имитирующих ПЭМИ РЭУ ОИ, модулированных информационным сигналом, – $\overline{\tau}_{cu}^{pr}$	$d_{1.2}^{(6)}$	10
	Выбор нарушителем режима работы РРП, обеспечивающего соответствие характеристикам перехватываемого сигнала ПЭМИ с целью выполнения условия (15), без применения мер защиты информации – $\overline{\tau}_{cu}$	$d_{2.2}^{(11)}$	4
	Выбор нарушителем режима работы РРП, обеспечивающего соответствие характеристикам перехватываемого сигнала ПЭМИ с целью выполнения условия (15), в условиях применения мер защиты информации – $\overline{\tau}_{cu}^{ext}$	$d_{2.2}^{(12)}$	4
	Выполнена проверка свойств перехваченной информации в соответствии с условиями (14)–(16) без применения мер защиты – $\overline{\tau}_{\text{ИПр}}^{*}$	$d_{\text{м}2}^{(Sp)}$	≈ 25
	Выполнена проверка свойств перехваченной информации в соответствии с условиями (14)–(16) в условиях применения мер защиты – $\tau_{\text{ИПр}}^{*\text{ЗИ}}$	$d_{\text{м}2}^{(Sp)}$	≈ 25



$$\mathbf{M}(\mathbf{D}_{1.1}) = \begin{bmatrix} & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & & + & & & & \\ 2 & & & + & & & \\ 3 & & & & + & & \\ 4 & & & & & + & \\ 5 & & & & & & + \end{bmatrix} \quad \mathbf{M}(\mathbf{D}_{2.1}) = \begin{bmatrix} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & & + & & & & & & & & & & \\ 2 & & & + & & & & & & & & & \\ 3 & & & & + & & & & & & & & \\ 4 & & & & & + & & & & + & & & \\ 5 & & & & & & + & & & & & & \\ 6 & & & & & & & + & & & & & \\ 7 & & & & & & & & + & & & & \\ 8 & & & & & & & & & & & & + \\ 9 & & & & & & & & & & + & & \\ 10 & & & & & & & & & & & + & \\ 11 & & & & & & & & & & & & + \end{bmatrix} \quad \mathbf{M}(\mathbf{D}_{3.1}) = \begin{bmatrix} & 1 & 2 & 3 \\ 1 & & + & \\ 2 & & & + \end{bmatrix}$$

Рис. 5. Функциональная модель процессов передачи информации на объекте информатизации, ее перехвата по ТКУИ за счет ПЭМИ РЭУ объекта и защиты информации от перехвата при параллельном выполнении действий, обеспечивающих их реализацию. В условиях применения адаптивных мер защиты

С учетом данных, приведенных в табл. 2, $\bar{\tau}_{ПрПИ} \approx 56$ мин, $\bar{\tau}_{ИПр} \approx 55$ мин. При этом среднее время перехвата информации в условиях применения адаптивных мер защиты составит $\bar{\tau}_{app}^{ЗИ} \approx 0$ мин. В этих условиях защищенность информации также можно считать обеспеченной.

На основе функциональных моделей, приведенных на рис. 5, могут быть получены лишь приближенные значения общих времен реализации параллельных процессов ИПр, ПрПИ и ПрЗИ.

Это обусловлено случайным характером времен выполнения действий в процессе реализации каждого из моделируемых процессов и экспертным способом их определения. Более того, неопределенность относительно вероятностных характеристик этих времен не позволяет получить адекватные оценки значений общих времен реализации указанных процессов и оценить защищенность информации в рассматриваемых условиях. При этом наличие множества логических условий достижения целей реализации этих процессов значительно усложняет решение задачи адекватной оценки защищенности информации.

Заключение

Представленные описательные и функциональные модели могут служить основой для разработки на основе аппарата сетей Петри–Маркова аналитических моделей оценки защищенности информации от ее утечки за счет ПЭМИ РЭУ ОИ в условиях динамики выполнения действий нарушителя и легитимных пользователей по реализации процессов перехвата и применения адаптивных мер защиты информации соответственно, учитывающих вероятностно-временной характер этих действий, выполняемых последовательно-параллельно при наличии определенных логических условий [28, 29], адекватно отражающих реализацию указанных процессов для конкретного ОИ и позволяющих получить аналитические соотношения для расчета показателей защищенности информации от утечки в условиях применения адаптивных мер защиты.

Литература

1. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст. – Режим доступа: http://docs.cntd.ru/docu-ment/gost-r-51275-2006.

2. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утв. приказом Гостехкомиссии России от 30.08.2002 № 282. – Режим доступа: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

3. 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]. – Режим доступа: https://base.garant.ru/70391358.

4. 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.: НПЦ «Аналитика», 2008. – 436 с.

5. Авсентьев О.С. Формирование обобщенного показателя ценности информации в каналах связи / О.С. Авсентьев, А.О. Авсентьев // Вестник Воронежского ин-та МВД России. – 2015. – № 3. – С. 55–63.

6. Авсентьев О.С. Математическая модель защиты информации от утечки по электромагнитным каналам / О.С. Авсентьев, А.Г. Вальде, А.Г. Кругов // Вестник Воронежского ин-та МВД России. – 2016. – № 3. – С. 42–50.

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

8. Оценка защищенности информационных процессов в территориальных органах внутренних дел: модели исследования / В.К. Джоган, А.С. Дерябин, В.С. Зарубин, В.В. Здольник, П.Е. Краснов, А.П. Курило, К.С. Скрыль, В.Н. Финько, А.Я. Фомин, А.А. Герасимов. – Воронеж: Воронежский институт МВД России, 2010. – 217 с.

9. Методический документ «Меры защиты информации в государственных информационных системах». Утв. ФСТЭК России 11 февраля 2014 г. – Режим доступа: fstec.ru

10. Авдеев В.Б. Сравнительная оценка методических подходов к расчёту отношения сигнал/шум в задачах контроля защищённости информации от утечки за счёт побочных электромагнитных излучений / В.Б. Авдеев, А.В. Анищенко // Специальная техника. – 2016. – № 1. – С. 54–63.

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

12. Вильямс Дж.Д. Совершенный стратег, или Букварь по теории стратегических игр / пер. с англ. Ю.С. Голубева–Новожилова; под ред. И.А. Полегаева. – М.: Советское радио, 1960. – 264 с.

13. Никольский Б.А. Основы радиотехнических систем: электрон. учебник / Самар. гос. аэрокосм. ун-т им. С.П. Королева (нац. исслед. ун-т). – Электрон. текстовые и граф. дан. (3,612 Мбайт). – Самара, 2013. – 1 эл. опт. диск (CD-ROM).

14. Теория электрической связи: учеб. пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.

15. Кубанов В.П. Влияние окружающей среды на распространение радиоволн. – Самара: ПГУТИ, 2013. – 92 с.

16. Авсентьев О.С. Модель оптимизации процесса передачи информации по каналам связи в условиях угроз ее безопасности / О.С. Авсентьев, В.В. Меньших, А.О. Авсентьев // Телекоммуникации. – 2016. – № 1. С. 28–32.

17. Авсентьев О.С. Исследование взаимосвязей между электрическими параметрами информационных сигналов при обосновании показателя защищенности информации от утечки по электромагнитным каналам / О.С. Авсентьев, А.О. Авсентьев, А.Г. Кругов // Вестник Воронежского ин-та МВД России. – 2017. – № 2. – С. 125–135.

18. Авсентьев О.С. Исследование условий возникновения технических каналов утечки информации по побочным электромагнитным излучениям на объектах информатизации / О.С. Авсентьев, А.О. Авсентьев, А.Г. Вальде // Вестник Воронежского ин-та МВД России. – 2017. – № 3. – С. 22–31.

19. 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.

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

21. Авсентьев А.О. Вербальная модель технического канала утечки информации за счет побочных электромагнитных излучений на объектах информатизации / А.О. Авсентьев, С.В. Пономаренко, А.Г. Кругов // Вестник Воронежского ин-та ФСИН России. – 2020. – № 1. – С. 9–21.

22. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера // Доклады ТУСУР. – 2014. – № 2. – С. 207–213.

23. Авсентьев О.С. Использование адаптационных методов для повышения защищенности информационных систем с направленными антеннами / О.С. Авсентьев, А.В. Золотухин, Р.В. Павлов, И.О. Плужникова, Н.Н. Толстых // Радиотехника. – 1999. – № 6. – С. 38–41.

24. Авдеев В.Б. К расчету уровней побочных электромагнитных излучений технических средств, входящих в состав персональных компьютеров // Телекоммуникации. – 2006. – № 2. – С. 40–44.

25. Авсентьев О.С. Обоснование показателя защищенности информации от утечки по электромагнитным каналам / О.С. Авсентьев, А.Г. Кругов // Доклады ТУСУР. – 2017. – Т. 20, № 1. – С. 59–64.

26. Авсентьев О.С. Структурно-логическое представление процесса передачи информации на объектах информатизации / О.С. Авсентьев, А.В. Заряев, А.Г. Кругов // Вестник ВИ МВД. – 2020. – №1. – С. 22–32.

27. Буравцев А. В. Стратифицированный метод построения сложной системы // Образовательные ресурсы и технологии. – 2017. – № 3 (20). – С. 23–32.

28. Игнатьев В.М. Сети Петри−Маркова / В.М. Игнатьев, Е.В. Ларкин. – Тула: ТулГТУ, 1994. – 163 с.

29. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов/н/Д: Изд-во СКНЦ ВШ, 2006. – 274 с.

Авсентьев Александр Олегович
Канд. техн. наук, ст. преп. каф. физики
Воронежского института МВД России
Патриотов пр-т, д. 53, г. Воронеж, Россия, 394065
Тел.: +7 (473-2) 00-52-66
Эл. почта: aoaao8787@mail.ru

Кругов Артем Геннадьевич
Гл. специалист центра информационных технологий,
связи и защиты информации УМВД России
по Тверской области
Мира пл., д. 1/70, г. Тверь, Россия, 170100
Тел.: +7 (482-2) 32-93-93
Эл. почта: krtemik@gmail.com

Перова Юлия Петровна
Ст. преп. института комплексной безопасности
и специального приборостроения РТИ-МИРЭА
Стромынка ул., д. 20, г. Москва, Россия, 107076
Тел.: +7 (499-6) 81-33-56
Эл. почта: julia_pn@pochta.ru

Avsentev A.O., Krugov A.G., Perova Yu.P.

Functional models of information protection against leakage due to spurious electromagnetic emissions of informatization objects

The authors consider an approach to construct functional models of information protection against leakage caused by spurious electromagnetic radiation of structural elements of informatization objects. The approach takes into account the dynamics of parallel processes of interception of this information by an intruder and its protection by legitimate users from interception in the application of adaptive protection measures, based on a stratified representation of aggregates actions performed during the implementation of these processes.

Keywords: functional model, information properties, information value, technical channel for information leakage, adaptive information protection measures, electrical characteristics of electronic devices, spurious electromagnetic radiation, conditions for matching heterogeneous characteristics.
doi: 10.21293/1818-0442-2020-23-2-17-35

References

1. GOST R 51275-2006. Protection of information. The object of informatization. Factors affecting information. General Provisions. Available at: http://docs.cntd.ru/document/gost-r-51275-2006 (Accessed: March 11, 2020) (in Russ.).

2. «Special requirements and recommendations for the technical protection of confidential information (STR-K)», approved by order of the State Technical Commission of Russia of August 30, 2002 No. 282. Available at: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm (Accessed: March 16, 2020) (in Russ.).

3. «About approval of requirements for the protection of information not constituting state secrets contained in state information systems»: Order of the State Technical Commission of Russia of February 11, 2013 No. 17. Available at: https://base.garant.ru/70391358 (Accessed: March 16, 2020) (in Russ.).

4. Khorev A.A. *Tekhnicheskaya zashchita in-formatsii: uchebnoye posobiye dlya studentov vuzov: v 3 t. T. 1: Tekhnicheskiye kanaly utechki informatsii* [Technical protection of information: a textbook for university students: 3 vols. vol. 1: Technical channels for information leakage]. Ed. Yu.N. Lavrukhina]. M.: SPC «Analytics», 2008. – 436 p. (in Russ.).

5. Avsentev O.S., Avsentev A.O. *Formirovaniye obobshchennogo pokazatelya tsennosti informatsii v kanalakh svyazi* [The formation of the information value generalized index in the communication channels]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2015, no. 3, pp. 55–63 (in Russ.).

6. Avsentiev O.S., Valde A.G., Krugov A.G. *Matematicheskaya model' zashchity informatsii ot utechki po elektromagnitnym kanalam* [The mathematical model of information protection from leakage through electromagnetic channel]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2016, no. 3, pp. 42–50 (in Russ.).

7. Avsentiev O.S., Krugov A.G., Shelupanov A.A. *Funktsional'nyye modeli protsessov realizatsii ugroz utechki informatsii za schet pobochnykh elektromagnitnykh izlucheniy ob"yektov informatizatsii* [Functional models of processes for realizing the threats of information leakage due to secondary electromagnetic emissions of objects of informatization]. *Proceedings of TUSUR University*, 2020, no. 1, pp. 29–39 (in Russ.).

8. Jogan V.K., Deryabin A.S., Zarubin V.S., Zdolnik V.V., Krasnov P.E., Kurilo A.P., Kurilo A.P., Skryl K.S., Finko V.N., Fomin A.Ya., Gerasimov A.A. *Otsenka zashchishchennosti informatsionnykh protsessov v territorial'nykh organakh vnutrennikh del: modeli issledovaniya : monografiya* [Security assessment of information processes in territorial internal affairs bodies: research models: monograph]. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 2010, 217 p. (in Russ.).

9. Methodical document «Information security measures in state information systems» approved by the State Technical Commission of Russia of February 11, 2014. Available at: fstec.ru (in Russ.).

10. Avdeev V.B., Anischenko A.V. *Sravnitel'naya otsenka metodicheskikh podkhodov k raschotu otnosheniya signal/shum v zadachakh kontrolya zashchishchonnosti informatsii ot utechki za schot pobochnykh elektromagnitnykh izlucheniy* [Comparative evaluation of methodological approaches to calculating the signal-to-noise ratio in the tasks of monitoring information security from leakage due to secondary electromagnetic radiation]. *Special Technique*, 2016, no. 1, pp. 54–63 (in Russ.).

11. Avdeev V.B., Katrusha A.N. *Raschot koeffitsiyenta oslableniya pobochnykh elektromagnitnykh izlucheniy* [Calculation of the coefficient of attenuation of secondary electromagnetic radiation]. *Special Technique*, 2013, no. 2, pp. 18–27 (in Russ.).

12. J.D. Williams *Sovershennyy strateg ili bukvar' po teorii strategicheskikh igr* [The perfect strategist or primer on the theory of strategic games] Translated from English by Yu.S. Golubeva – Novozhilova edited by I.A. Polegaeva. M.: Publishing house «Soviet Radio», 1960. 264 p. (in Russ.).

13. Nikolsky, B. A. *Osnovy radiotekhnicheskikh sistem* (*elektron. Uchebnik*) [Fundamentals of radio systems (electron. textbook) [Electronic resource] Ministry of Education and Science of Russia, Samar. state aerospace. un-t them. S.P. Koroleva (National Research University). The electron. text and graph. Dan. (3.612 MB), Samara, 2013, 1 opt. disk (CD-ROM) (in Russ.).

14. Vasiliev K.K., Glushkov V.A., Dormidontov A.V., Nesterenko A.G. *Teoriya elektricheskoy svyazi: uchebnoye posobiye* [Theory of electrical communication: a training manual].; under the general. ed. K.K. Vasilieva. Ulyanovsk: UlSTU, 2008. 452 p. (in Russ.).

15. Kubanov V.P. *Vliyaniye okruzhayushchey sredy na rasprostraneniye radiovoln* [The influence of the environment on the propagation of radio waves]. Samara: PSUTI, 2013. 92 p. (in Russ.).

16. Avsentev O.S., Menshikh V.V., Avsentev A.O. *Model' optimizatsii protsessa peredachi informatsii po kanalam svyazi v usloviyakh ugroz yeye bezopasnosti* [Process optimization model of information transfer through communication channels under threat conditions for its security]. *Telecommunications*, 2016, no. 1, pp. 28–31 (in Russ.).

17. Avsentev O.S., Avsentev A.O., Krugov A.G. *Issledovaniye vzaimosvyazey mezhdu elektricheskimi parametrami informatsionnykh signalov pri obosno-vanii pokazatelya zashchishchennosti informatsii ot utechki po elektromagnitnym kanalam* [The research of the interrelationships between electrical parameters of information signals in the justification of increased security against leakage of information by electromagnetic channels]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2017, no. 2, pp. 125–135 (in Russ.).

18. Avsentev O.S., Avsentev A.O., Valde A.G. *Issledovaniye usloviy vozniknoveniya tekhnicheskikh kanalov utechki informatsii po pobochnym elektromagnitnym izlucheniyam na ob"yektakh informatizatsii* [Investigation of the conditions for the occurrence of technical channels for information leakage due to spurious electromagnetic radiation at information objects]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2017, no. 3, pp. 22–31 (in Russ.).

19. Menshakov Yu. K. *Teoreticheskiye osnovy tekhnicheskikh razvedok : ucheb. posobiye* [Theoretical foundations of technical intelligence: textbook. Allowance. ed. Yu.N. Lavrukhina]. M.: Publishing House of MSTU. N.E. Bauman, 2008. 536 p. (in Russ.).

20. Antipov D.A., Shelupanov A.A. *Issledovaniye napravlennosti pobochnogo elektromagnitnogo izlucheniya ot personal'nogo komp'yutera* [A study of the direction of incidental electromagnetic radiation from a personal computer]. *Proceedings of TUSUR University*, 2018, no. 2, pp. 33–37 (in Russ.).

21. Avsentiev A.O., Ponomarenko S.V., Krugov A.G. *Verbal'naya model' tekhnicheskogo kanala utechki informatsii za schet pobochnykh elektromagnitnykh izlucheniy na ob"yektakh informatizatsii* [Verbal model of the technical channel of information leakage due to spurious electromagnetic radiation at informatization facilities]. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*, 2020, no. 1, pp. 9–21 in Russ.).

22. Khorev A.A. *Otsenka vozmozhnosti obnaruzheniya pobochnykh elektromagnitnykh izlucheniy videosistemy komp'yutera* [Assessment of the possibility of detecting incidental electromagnetic radiation of a computer video system]. *Proceedings of TUSUR University*, 2014, no. 2, pp. 207–213 (in Russ.).

23. Adaptive methods using for protection improvement of informational system with narrow radiation pattern. Avsent'ev O.S., Zolotukhin A.V., Pavlov R.V., Pluzhnikova I.O., Tolstykh N.N. *Radio engineering*, 1999, no. 6, pp. 38–41 (in Russ.).

24. Avdeev V.B. *K raschetu urovney pobochnykh elektpomagnitnykh izlucheniy tekhnicheskikh spedstv, vkhodyashchikh v sostav pepsonal'nykh komp'yutepov* [To the calculation of the level of spurious electromagnetic emissions of technical equipment that are part of personal computers]. *Telecommunications*, 2006, no. 2, pp. 40–44 (in Russ.).

25. Avsentev O.S., Krugov A.G. *Obosnovaniye pokazatelya zashchishchennosti informatsii ot utechki po elektromagnitnym kanalam* [Rationale for increased DLP index to protect information from leakage via electromagnetic channels]. *Proceedings of TUSUR University*, 2017, vol. 20, no. 1, pp. 59–64 (in Russ.).

26. Avsentiev O.S., Zaryaev A.V., Krugov A.G. *Strukturno-logicheskoye predstavleniye protsessa peredachi informatsii na ob"yektakh informatizatsii* [Structural-logical representation of the process of information transfer on objects of in-formatization]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2020, no.1 pp. 22–32 (in Russ.).

27. Buravtsev A. V. *Stratifitsirovannyy metod postroyeniya slozhnoy sistemy* [A stratified method for constructing a complex system]. Educational resources and technologies, 2017, no. 3 (20), pp. 23–32 (in Russ.).

28. Ignatiev, V.M. *Seti Petri−Markova* [Petri – Markov networks]. Tula: TulGTU, 1994, 163 p. (in Russ.).

29. Yazov Y.K. *Osnovy metodologii koli-chestvennoy otsenki effektivnosti zashchity in-formatsii v komp'yuternykh sistemakh* [Fundamentals of the methodology for the quantitative assessment of the effectiveness of the protection of information in computer systems]. Rostov-on-Don, Publishing House SKNTs VSh, 2006, 274 p. (in Russ.).

Alexander O. Avsentev
Candidate of Engineering Sciences.
Senior Lecturer of the chair of Physics
Voronezh Institute of the Ministry of Internal Affairs of Russia
53, Patriotov pr., Voronezh, Russia, 394065
Phone: +7 (473-2) 00-52-66
E-mail: aoaao8787@mail.ru

Artem G. Krugov
Chief specialist of the center of information technology,
communications and information protection.
Ministry of Internal Affairs of Russia in the Tver region
1, Mira sq., 70, Tver, Russia, 170100
Phone: +7 (482-2) 32-93-93
E-mail: krtemik@gmail.com

Yulia P. Perova
Senior Lecturer
Institute for Integrated Security and Special Instrumentation
RTI-MIREA
20, Stromynka st., Moscow, Russia, 107076
Phone: +7 (499-6) 81-33-56
E-mail: ulia_pn@pochta.ru