УДК 004.056:519.1

О.С. Авсентьев, А.Г. Кругов, П.А. Шелупанова

Функциональные модели процессов реализации угроз утечки информации за счет побочных электромагнитных излучений объектов информатизации

Рассматривается подход к построению функциональных моделей процессов реализации угроз утечки информации за счет побочных электромагнитных излучений радиоэлектронных устройств объектов информатизации, основанный на стратифицированном представлении таких процессов, отражающем связь между действиями нарушителя, выполняемыми на разных стратах описания в виде совокупности действий, соответствующих каждому из возможных вариантов реализации процессов рассматриваемого типа.

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

doi: 10.21293/1818-0442-2020-23-1-29-39

Объект информатизации (ОИ) – это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [1].

Использование ОИ рассматриваемого типа в различных сферах деятельности при обеспечении взаимодействия организаций, предприятий, а также организаций государственного сектора позволяет значительно повысить эффективность деятельности этих организаций. По решаемым задачам и выполняемым функциям ОИ организаций государственного сектора имеют ряд особенностей, обусловленных в первую очередь тем, что на этих объектах обрабатывается и передается информация государственного значения, подлежащая защите от угроз нарушения ее безопасности. В качестве основных факторов, обусловливающих возможность реализации этих угроз, следует отметить использование для реализации информационных процессов по обработке и передаче информации на ОИ сигналов различной физической природы. Кроме того, применение в структуре ОИ технических средств (ТС) на основе различного рода радиоэлектронных устройств (РЭУ) обусловливает излучения сигналов, функционально присущие этим ТС, а также побочные электромагнитные излучения (ПЭМИ) элементов этих ТС и ПЭМИ, модулированные информативным сигналом, сопровождающим работу РЭУ [1].

Указанные особенности обработки информации на ОИ обусловливают определенную направленность угроз ее безопасности на противоправные действия по реализации технических каналов утечки информации (ТКУИ) за счет ПЭМИ РЭУ ОИ и применение мер защиты, учитывающих динамику указанных действий.

Динамика противоправных действий заключается в следующем.

Выбор РЭУ в составе ТС ОИ осуществляется в процессе проектирования и разработки объекта (до начала эксплуатации) с учетом его назначения, вида обрабатываемой (подлежащей передаче) информации при обеспечении свойств, характеризующих ее ценность для легитимных пользователей, как обеспечивающего ресурса их деятельности [2]. Реализация процессов обработки и передачи информации (далее – информационных процессов (ИПр)) на ОИ осуществляется после ввода объекта в эксплуатацию. При этом временные характеристики реализации этих процессов (начало, продолжительность, окончание) носят случайный характер.

В соответствии с определением, приведенным в [3], ТКУИ включает источник (датчик) информации (ДИ), среду распространения информативного сигнала и разведывательный приемник, как техническое средство разведки (ТСР). При этом ДИ и часть среды распространения информативного сигнала располагаются в пределах контролируемой зоны (КЗ) ОИ. Остальные элементы ТКУИ могут располагаться как за пределами КЗ, так и в смежных с ОИ помещениях в пределах общей КЗ [4]. В условиях неопределенности относительно характеристик ИПр в процессе реализации ТКУИ нарушителем осуществляется выбор ТСР и места его применения с целью обеспечения свойств перехватываемой информации, характеризующих ее ценность для нарушителя и удовлетворяющих его требованиям.

До настоящего времени описательные модели процессов реализации ТКУИ, возникающих за счет ПЭМИ РЭУ ТС ОИ в условиях динамики их реализации нарушителем, не разрабатывались. Указанные обстоятельства практически исключают возможность учета этой динамики при обеспечении защиты информации на ОИ, что приводит к искажению результатов оценки ее защищенности от утечки. Это обусловлено большим количеством подлежащих учету характеристик сигналов как материальных носителей информации в пределах ОИ и в ТКУИ, характеристик РЭУ, используемых для обработки и пе-

редачи этих сигналов на ОИ, условий согласования этих характеристик и сложностью их вербального описания. Кроме того, в интересах количественной оценки защищенности информации от утечки возникает необходимость формирования в рамках таких моделей исходных данных, характеризующих динамику реализации таких ТКУИ. Это, в свою очередь, обусловливает необходимость разработки соответствующих формализованных функциональных моделей ИПр как объекта защиты и процесса реализации ТКУИ рассматриваемого типа.

Общее описание угроз утечки информации по техническим каналам за счет ПЭМИ РЭУ ОИ

Угрозы утечки информации по техническим каналам за счет ПЭМИ РЭУ ОИ – это угрозы безопасности информации, связанные с реализацией нарушителем ТКУИ, возникающих за счет ПЭМИ РЭУ в составе ТС ОИ.

Рассмотрим элементы описания ТКУИ рассматриваемого типа.

К основным элементам описания такого рода ТКУИ относятся: РЭУ в составе ТС ОИ, используемые в качестве ДИ (источника информации в структуре ТКУИ), воздушная среда распространения информативного сигнала и разведывательные радиоприемники (РРП).

В составе ТС на ОИ для реализации ИПр применяются различные РЭУ. При этом в целях обеспечения свойств обрабатываемой (передаваемой) информации, характеризующих ее ценность для легитимных пользователей и удовлетворяющих требованиям обеспечиваемой деятельности, на ОИ формируется некоторая траектория, включающая различные РЭУ [5, 6]. Каждое РЭУ в этой траектории является источником ПЭМИ широкого частотного диапазона. Как отмечено в [7], характер этих излучений определяется назначением, схемными решениями, мощностью, материалами и конструкцией устройства. При прохождении информационных сигналов через РЭУ ОИ по выбранной траектории возникают ПЭМИ этих РЭУ, модулированные информативным (опасным) сигналом, которые могут быть использованы в качестве материальных носителей перехватываемой нарушителем при помощи РРП информации по возникающему при этом ТКУИ [8, 9].

В связи с особенностями функционирования ОИ, обусловленными разнообразием номенклатуры и разнородностью РЭУ, используемых в составе ТС ОИ, а также наличием многофакторных взаимосвязей между этими РЭУ у нарушителя появляется возможность реализации множества таких ТКУИ, имеющих различные характеристики [8]. Данное обстоятельство связано, с одной стороны, с отсутствием у нарушителя возможности какого-либо влияния на структуру и условия функционирования ОИ и их РЭУ, с другой стороны, с отсутствием у легитимных пользователей ОИ возможности определения действий нарушителя в процессе реализации ТКУИ.

Нарушитель при выполнении этих действий руководствуется принципами ведения технической разведки (ТР), приведенными в [7].

В связи с тем, что передача информации по основному каналу связи между легитимными пользователями ограничена во времени, для него важное значение имеет реализация принципа оперативности ведения ТР, предполагающего динамичность процесса реализации перехвата и доставки информации в центр ее сбора и обработки. При этом ведение ТР может осуществляться с учетом динамики изменения обстановки, связанной с применением на ОИ мер защиты информации и различными условиями распространения информативных сигналов.

В структуре ТКУИ РЭУ в составе ТС ОИ используются в качестве физических преобразователей. Знание физических принципов действия такого рода преобразователей позволяет решать задачу определения характеристик побочных физических полей, образующих ТКУИ, и согласования характеристик этих полей с характеристиками РРП, используемых для перехвата информативных сигналов.

Для реализации процесса перехвата информации (ПрПИ) по ТКУИ нарушителю необходимо учитывать сведения об обрабатываемой на ОИ информации, о структуре и закономерностях функционирования ТС объекта, об используемых схемных и технологических решениях, о методах, способах и мерах защиты информации. С учетом этих сведений осуществляется выбор места расположения, тип и режимы работы РРП в целях обеспечения требований к свойствам перехватываемой информации.

Следует отметить важные обстоятельства, связанные с разнородностью обрабатываемой на ОИ информации, различиями характеристик используемых для этих целей РЭУ в составе ТС, а также их взаимосвязями в структуре ОИ, обусловливающие различные условия распространения ПЭМИ [10–12].

Как показано в [8], ТКУИ может быть представлен в виде типовой радиотехнической системы, представленной на рис. 1, где используются следующие обозначения: ДИ и ПИ – датчик и получатель информации; ПрУ и ОПрУ – преобразующее и обратное преобразующее устройства; ПРД и ПРМ – передающее и приемное устройства; АФУ ПРД и АФУ ПРМ – передающее и приемное антенно-фидерные устройства; ВС – воздушная среда распространения информативного сигнала [13].

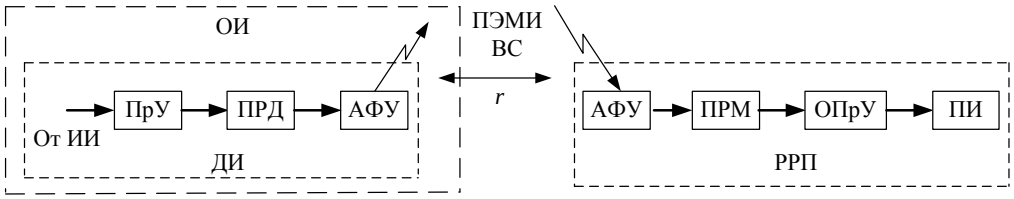

Рис. 1. Структура технического канала утечки информации за счет ПЭМИ

Обширную номенклатуру ДИ могут составлять микрофоны телефонных аппаратов, мониторы и оборудование средств вычислительной техники (СВТ), накопители, периферийные устройства, различные РЭУ в составе каналообразующей аппаратуры и др. [1, 4, 7].

На пути от ДИ до ПИ в различных элементах траектории реализации ТКУИ возможны преобразования сигналов из одного вида в другой. При этом ПЭМИ различных РЭУ в структуре ОИ могут иметь различные характеристики. Указанные обстоятельства также обусловливают определенные трудности для нарушителя по реализации действий, выполняемых с целью формирования ТКУИ рассматриваемого типа, связанные с выбором РРП и определением места его применения.

Для того чтобы какое-либо РЭУ могло использоваться в качестве ДИ в структуре ТКУИ, оно должно иметь соответствующие характеристики [7].

ДИ содержит элемент, чувствительный к информационным сигналам перехватываемой информации определенного вида (речевой, документальной, телекоммуникационной) в различной форме представления (акустические колебания, колебания электрического тока в аналоговом или цифровом виде). На выходе этого элемента (ПрУ, см. рис. 1) формируется электрический сигнал, модулированный информационным сигналом, поступающим от ИИ [7].

Кроме того, такой ДИ содержит элементы ПРД (с разрешающей способностью, линейностью, полосой частот и инерционностью), обеспечивающие формирование ПЭМИ, а также проводники, выполняющие роль антенно-фидерных устройств (АФУ). В качестве АФУ могут использоваться и проводники, соединяющие различные РЭУ в составе ТС ОИ. От конструктивных особенностей элементов ДИ, выполняющих роль АФУ, зависит вид диаграммы направленности ПЭМИ. Так, в [11] показано, что диаграмма направленности ПЭМИ компьютера отличается от круговой. Данное обстоятельство также может учитываться нарушителем при определении направления максимального уровня излучения ПЭМИ с целью выбора места расположения РРП, включающего АФУ, ПРМ, ОПрУ и устройство отображения перехватываемой информации (ПИ).

При этом характеристики этого РРП должны соответствовать характеристикам принимаемых сигналов ПЭМИ. В качестве электрических характеристик РРП рассматриваются $\mu_{РРП}$ чувствительность к принимаемым сигналам ПЭМИ, полоса пропускания $\Delta F_{РРП}$ и время обеспечения приема $\Delta\tau_{РРП}$. Основными характеристиками сигнала ПЭМИ при этом являются отношение сигнал / шум, $A_{ПЭМИ}$ / $P_{ш}$ на входе РРП, ширина спектра частот $\Delta f_{ПЭМИ}$ и время $\Delta\tau_{ПЭМИ}$, в течение которого ПЭМИ с такими характеристиками может использоваться в качестве материального носителя перехватываемой информации. Условия согласования определяются в соответствии с [14, 15]:

$$A_{ПЭМИ}/P_{ш} \geq \mu_{РРП}, \quad (1)$$

$$\Delta F_{РРП} \geq \Delta f_{ПЭМИ}, \quad (2)$$

$$\Delta\tau_{РРП} \geq \Delta\tau_{ПЭМИ}. \quad (3)$$

На рис. 1 показано, что ДИ и часть воздушной среды распространения сигнала ПЭМИ располагаются в пределах КЗ ОИ и нарушитель не имеет возможности влияния на характеристики сигнала ПЭМИ в пределах этой зоны. Поэтому основными элементами, которыми может манипулировать нарушитель в процессе реализации ТКУИ, являются характеристики ВС среды распространения ПЭМИ за пределами ОИ и характеристики элементов РРП.

Сигналы при распространении в физической среде ослабляются. Ослабление ПЭМИ при его распространении в воздушной среде зависит от частоты излучения, типа трассы, расстояния r (зоны) от излучателя и характеризуется коэффициентом ослабления $K_o(r)$ [16], а также условиями распространения такого рода сигналов [17]. Известно множество подходов к расчету $K_o(r)$ в различных условиях распространения радиоволн [18]. В [16], например, приведены как приближенная «трехзонная», так и точные формулы для коэффициента ослабления ПЭМИ $K_o(r)$ по электрическому и магнитному полю. Однако в этих формулах не учитывается динамика процесса реализации ТКУИ, реализуемого нарушителем с целью перехвата информации.

В интересах исследования динамики процесса реализации ТКУИ рассмотрим приведенное в [17] выражение для определения радиочастотной энергетики радиолинии в условиях свободного пространства:

$$P_2 = (P_1 \cdot \eta_1 \cdot \eta_2 \cdot G_1 \cdot G_2 \cdot \lambda^2)/(4\pi r^2), \quad (4)$$

где P_1 и P_2 – мощности радиосигнала на выходе ПРД и на входе ПРМ соответственно; η_1 и η_2 – коэффициенты полезного действия фидеров передающей и приемной антенн соответственно; $G_1 = D_1 \cdot \eta_{A1}$ и $G_2 = D_2 \cdot \eta_{A2}$ – коэффициенты усиления передающей и приемной антенн соответственно; η_{A1} и η_{A2} – коэффициенты направленного действия антенн; λ – длина волны электромагнитного излучения; r – расстояние между передающей и приемной антеннами.

Для ТКУИ, структура которого приведена на рис. 1, выражение (4) запишем в виде

$$P_2 = P_1 \cdot K_o(r), \quad (5)$$

где $K_o(r) = (\eta_1 \cdot \eta_2 \cdot G_1 \cdot G_2 \cdot \lambda^2)/(4\pi r^2)$ – коэффициент ослабления сигнала ПЭМИ по мощности на пути распространения от ДИ до входного устройства ПРМ РРП.

Основными особенностями ПЭМИ в ТКУИ рассматриваемого типа являются:

– излучатели ПЭМИ могут быть точечными и распределенными [3, 7];

– ПЭМИ этих излучателей могут распространяться в однородной и в неоднородной среде. При этом диаграмма направленности ПЭМИ может отличаться от круговой [11];

– возможны отражения (переотражения) ПЭМИ от физических объектов и неоднородностей среды на пути их распространения [17].

Указанные особенности обусловливают динамику процесса реализации нарушителем ТКУИ за счет ПЭМИ РЭУ ТС ОИ.

Условия (1) и (2) на входе ПРМ могут выполняться частично или вообще не выполняться.
Так, вид и характеристики (временные, энергетические и спектральные) излучаемого ПЭМИ в существенной степени определяются видом обрабатываемой на ОИ информации (речевая, документальная, телекоммуникационная) (массивы $м_i$) [7]. При этом в качестве ДИ в ТКУИ могут использоваться только РЭУ ТС ОИ, чувствительные к проходящим через них информационным сигналам соответствующего массива $м_i$. Геометрические размеры ДИ как излучателей ПЭМИ, а также соединяющих их проводников как своего рода микроантенн, определяют направленность излучения и его энергетику (η_1, G_1, P_1) [19].

Вид диаграммы направленности излучения в существенной степени зависит от его частотного спектра и конструктивных особенностей РЭУ ОИ. Эта зависимость определяется соотношением геометрических размеров АФУ излучателей ПЭМИ ($D_{ПЭМИ}$) и длины волны (спектра) излучения ($\lambda_{ПЭМИ}$). При $D_{ПЭМИ} < \lambda_{ПЭМИ}/2$ нарушаются условия согласования излучателя ПЭМИ со средой их распространения и диаграмма направленности излучения близка к круговой. При $D_{ПЭМИ} \geq \lambda_{ПЭМИ}/2$ направленность излучения определяется расположением излучателя в пространстве и может отличаться от круговой. С увеличением частоты $f_{ПЭМИ}$ эта зависимость проявляется все в большей степени [19]. Это приводит к необходимости поиска нарушителем места для расположения РРП с целью определения направления максимальной мощности излучения ПЭМИ. В условиях неопределенности нарушителя относительно структурных элементов ОИ поиск места размещения РРП может занять достаточно много времени. Место применения РРП в процессе реализации ТКУИ определяется в зависимости от расстояния *r* с учетом выполнения условия (1), а выбор типа РРП осуществляется с учетом выполнения условия (2). При этом проверка выполнения условий (1) и (2) требует времени. Указанные обстоятельства обусловливают динамику процесса реализации нарушителем ТКУИ рассматриваемого типа. В этих условиях будем считать процесс ПрПИ перехвата информации реализованным при выполнении условия (3).

В свою очередь, условие (3) будем считать выполненным при одновременном выполнении условий (1) и (2). При этом действия нарушителя по выполнению этих условий могут происходить как последовательно, так и параллельно, а времена их выполнения являются случайными.

Следует отметить, что процесс ПрПИ перехвата информации может быть реализован только тогда, когда сигнал, воздействующий на ДИ, является носителем информации и ИПр информационный процесс на ОИ реализуется.

В связи с неопределенностью нарушителя относительно временных характеристик ИПр время его реализации определим как сумму времен τ_{st} по настройке ТС ОИ в штатном режиме, τ_{ex} ожидания передачи и τ_{tr} передачи информации на ОИ:

$$\tau_{ИПр} = \tau_{st} + \tau_{ex} + \tau_{tr}. \quad (6)$$

В соответствии с рассмотренными ранее действиями нарушителя по реализации ТКУИ за счет ПЭМИ РЭУ ОИ время $\tau_{ПрПИ}$ реализации процесса перехвата информации определим как сумму времен $\tau_{(1)}$ и $\tau_{(2)}$ реализации действий, направленных на выполнение условий (1) и (2) (при последовательном или параллельном их выполнении) и времени τ_{app} перехвата информации:

$$\tau_{ПрПИ} = \tau_{(1)} + \tau_{(2)} + \tau_{app}, \quad (7)$$

$$\tau_{ПрПИ} = \max(\tau_{(1)}, \tau_{(2)}) + \tau_{app}. \quad (8)$$

При этом время $\tau_{(1)}$ включает время τ_{pl} выбора места применения РРП с точки зрения скрытности (в соответствии с r_{min} минимально возможным расстоянием до КЗ), время τ_{in} сканирования по частоте, время τ_{dir} определения направления максимального уровня излучения (диаграммы направленности АФУ ДИ) и время τ_{cor} корректирования места применения РРП (с учетом расстояния *r*), обеспечивающего выполнение условия (1). С учетом последовательного выполнения этих действий запишем:

$$\tau_{(1)} = \tau_{pl} + \tau_{in} + \tau_{dir} + \tau_{cor}. \quad (9)$$

Время $\tau_{(2)}$ включает время τ_{mod} выбора режима работы РРП и время τ_{cu} настройки этого режима с учетом спектра сигнала ПЭМИ:

$$\tau_{(2)} = \tau_{mod} + \tau_{cu}. \quad (10)$$

Перехват информации считается успешным при выполнении условий:

$$\tau_{(1)} + \tau_{(2)} < \tau_{ИПр}. \quad (11)$$

$$\tau_{app} > \overset{*}{\tau}_{ИПр}, \quad (12)$$

$$\overset{*}{\tau}_{ИПр} \geq \tau^{тр}_{ИПр}, \quad (13)$$

где $\overset{*}{\tau}_{ИПр} = \tau_{ИПр} \cdot K_{ИПр}$, $0 \leq K_{ИПр} \leq 1$; $K_{ИПр}$ – коэффициент, характеризующий часть перехваченной информации ИПр при выполнении условий (1) и (2); $\tau^{тр}_{ИПр}$ – часть информационного процесса, перехват информации в которой удовлетворяет требованиям нарушителя.

Легитимным пользователям для защиты информации от утечки за счет ПЭМИ ТС ОИ необходимо применять меры защиты в целях противодействия реализации нарушителем ТКУИ рассматриваемого типа.

С учетом (11) – (13) условие обеспечения защиты информации от утечки запишем в виде

$$(\tau_{(1)} + \tau_{(2)}) > (1 - K_{\text{ИПР}}) \cdot \tau_{\text{ИПр}}. \qquad (14)$$

На рис. 2 и 3 представлены временные диаграммы выполнения нарушителем действий в соответствии с выражениями (7) и (8).

Таким образом, реализация угрозы утечки информации по ТКУИ за счет ПЭМИ РЭУ ОИ от начала ее реализации до момента окончания перехвата информации определяется суммарным временем выполнения каждого действия, в совокупности составляющих процесс ПрПИ с учетом обеспечения выполнения условия (3).

Значения временных характеристик всех действий, приведенных на рис. 3 и 4, случайны. Однако усредненные их значения могут быть определены либо экспертным путем, либо с использованием сведений о технических характеристиках ТС и РРП, применяемых для реализации процессов ИПр и ПрПИ.

В табл. 1 приведены примерные значения временных характеристик действий, составляющих процессы ИПр и ПрПИ для выделенного помещения, предназначенного для проведения мероприятий с применением ТС звукоусиления и связи для передачи речевой информации.

В описательной модели процесса реализации угрозы утечки информации по техническим каналам за счет ПЭМИ РЭУ ОИ могут быть учтены штатные меры защиты информации, реализуемые в процессе проектирования ОИ, такие как экранирование и заземление экранов РЭУ и соединительных линий ТС, ограничение уровней информационных сигналов, предаваемых через структурные элементы ОИ, и др. Применение этих мер позволит снизить уровень ПЭМИ, что, в свою очередь, может привести к увеличению временных характеристик действий нарушителя, направленных на обеспечение выполнения условий (1) и (2) при реализации процесса ПрПИ.

Наряду с временными характеристиками, приведенными в табл. 1, в описательной модели должны быть представлены и амплитудно-частотные характеристики информационных сигналов, используемых для передачи информации по траектории РЭУ ОИ и обусловливающих соответствующие характеристики ПЭМИ этих РЭУ, энергетику радиолинии в ТКУИ и возможность обеспечения требований нарушителя к свойствам перехватываемой информации. В рамках описательной модели устанавливаются также соответствия характеристик информативных сигналов ПЭМИ и РРП, обеспечиваемые при выполнении противоправных действий, связанных с условиями (1) и (2).

При описании угрозы рассматриваемого типа может быть указан способ преодоления меры защиты. В качестве недостатков такой модели следует отметить следующие: отсутствие детализации выполняемых нарушителем действий, характеризующей возможность такой реализации; сложность учета применения дополнительных мер защиты организационного, оперативного или оперативно-технического характера, направленных на локализацию действий нарушителя по обнаружению ПЭМИ и определению места применения РРП.

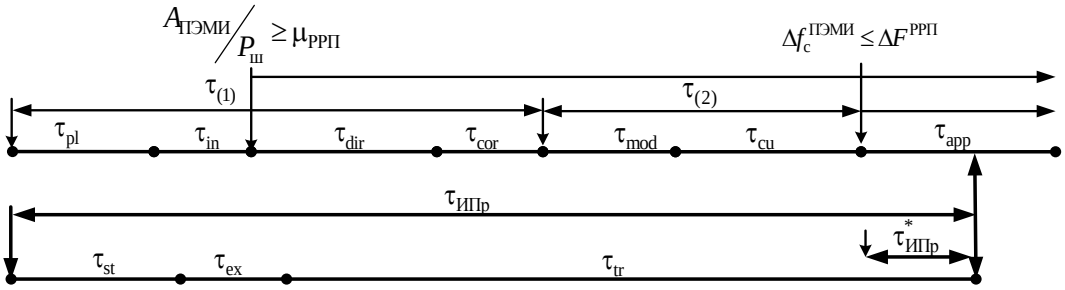

Рис. 2. Временные диаграммы процессов передачи информации на объекте информатизации и реализации ТКУИ при последовательном выполнении действий, обеспечивающих реализацию

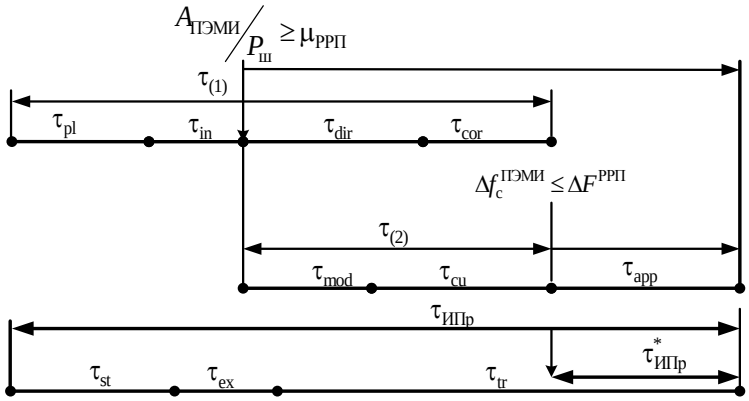

Рис. 3. Временные диаграммы процессов передачи информации на объекте информатизации и реализации ТКУИ при параллельном выполнении действий, обеспечивающих реализацию

Таблица 1

Временные характеристики действий, составляющих процессы ИПр и ПрПИ

№ п/п	Название характеристики и ее обозначение	Способ определения	Минимальное значение, мин	Максимальное значение, мин	Среднее значение, мин
1	Время настройки ТС ОИ в заданном режиме – τ_{st}	Технические характеристики ТС	10	15	12,5
2	Время ожидания передачи – τ_{ex}	Эксперт	5	10	7,5
3	Время передачи информации на ОИ – τ_{tr}	Эксперт (на основе регламента)	30	40	35
4	Время работы РРП в режим сканирования по частоте – τ_{in}	Технические характеристики РРП	8	12	10
5	Время определения направления максимального уровня излучения – τ_{dir}	Эксперт	5	7	6
6	Время определения места применения РРП – τ_{ch}	Эксперт	6	10	8
7	Время выбора режима работы РРП – τ_{mod}	Технические характеристики РРП	1	2	1,5
8	Время настройки РРП в выбранном режиме – τ_{cu}	Технические характеристики РРП	2	3	2,5
9	Часть информационного процесса, перехват информации, в которой удовлетворяет требованиям нарушителя, – $\tau_{ИПр}^{тр}$	Эксперт	1,5	2	1,75

Сведения, содержащиеся в описательной модели процессов реализации угроз утечки информации по техническим каналам за счет ПЭМИ РЭУ ОИ, служат основой для разработки функциональных моделей этих процессов и используются при разработке моделей оценки защищенности информации на ОИ.

Следует отметить, что невозможно разработать единую модель оценки защищенности информации на ОИ различного назначения. Для каждого объекта и применяемой меры защиты информации (штатной или дополнительной) необходимо разрабатывать оригинальную модель. При этом, поскольку для различных ОИ состав и последовательность действий, выполняемых нарушителем в процессе реализации ТКУИ рассматриваемого типа в условиях применения легитимными пользователями разных мер защиты, отличается, то функциональные модели процесса реализации угрозы также отличаются.

Функциональные модели процессов реализации угроз утечки информации за счет побочных электромагнитных излучений радиоэлектронных устройств объектов информатизации

Для оценки возможностей реализации угроз рассматриваемого типа с учетом временного фактора для конкретного ОИ необходимо определить время выполнения действий, составляющих процесс реализации угрозы, и их последовательность. Применительно к угрозам утечки информации по ТКУИ, возникающим за счет ПЭМИ РЭУ ОИ, такие модели ранее не разрабатывались. Характеристика действий, выполняемых в ходе реализации процессов перехвата информации по ТКУИ рассматриваемого типа, давалась без детализации условий их выполнения в ходе моделирования с использованием аппарата марковских [20], полумарковских процессов [21] и сетей Петри–Маркова [22] в виде описаний соответствующих схем. Функциональные модели процессов реализации угроз утечки информации по ТКУИ рассматриваемого типа с учетом этих условий также не разрабатывались.

В данной работе предложен подход к разработке такого рода функциональных моделей, основанный на стратифицированном представлении таких процессов (рис. 4) с выделением уровней (этапов) реализации и определением связей между ними в структуре ТКУИ в целом [23, 24].

При таком представлении обеспечивается возможность отражения связей между действиями, выполняемыми на разных стратах описания моделируемого процесса, и по аналогии с [24] может быть сформирована совокупность действий для каждого возможного варианта реализации ТКУИ за счет ПЭМИ РЭУ ОИ. В результате выполнения действий на всех стратах создаются условия для отображения перехваченной информации в устройстве отображения ПИ.

На страте 1 осуществляются действия по выбору места применения РРП с учетом обеспечения r_{min} минимально возможного расстояния до КЗ.

Страта 2 соответствует обнаружению ПЭМИ различных РЭУ в структуре ОИ, используемых в качестве ДИ в ТКУИ, путем применения имеющихся РРП в режиме сканирования диапазона частот.

При этом выполняется условие (1), но возможно, что не выполняется условие (2), поскольку характеристики выбранного режима работы РРП могут не соответствовать характеристикам сигнала ПЭМИ.

Следующая страта соответствует действиям по определению направления максимального уровня ПЭМИ с использованием АФУ направленного действия в составе РРП. При этом возможно корректирование в соответствии с расстоянием r от ДИ места применения РРП с последующим (или параллельным) выбором режима работы РРП с целью обеспечения выполнения условия (2).

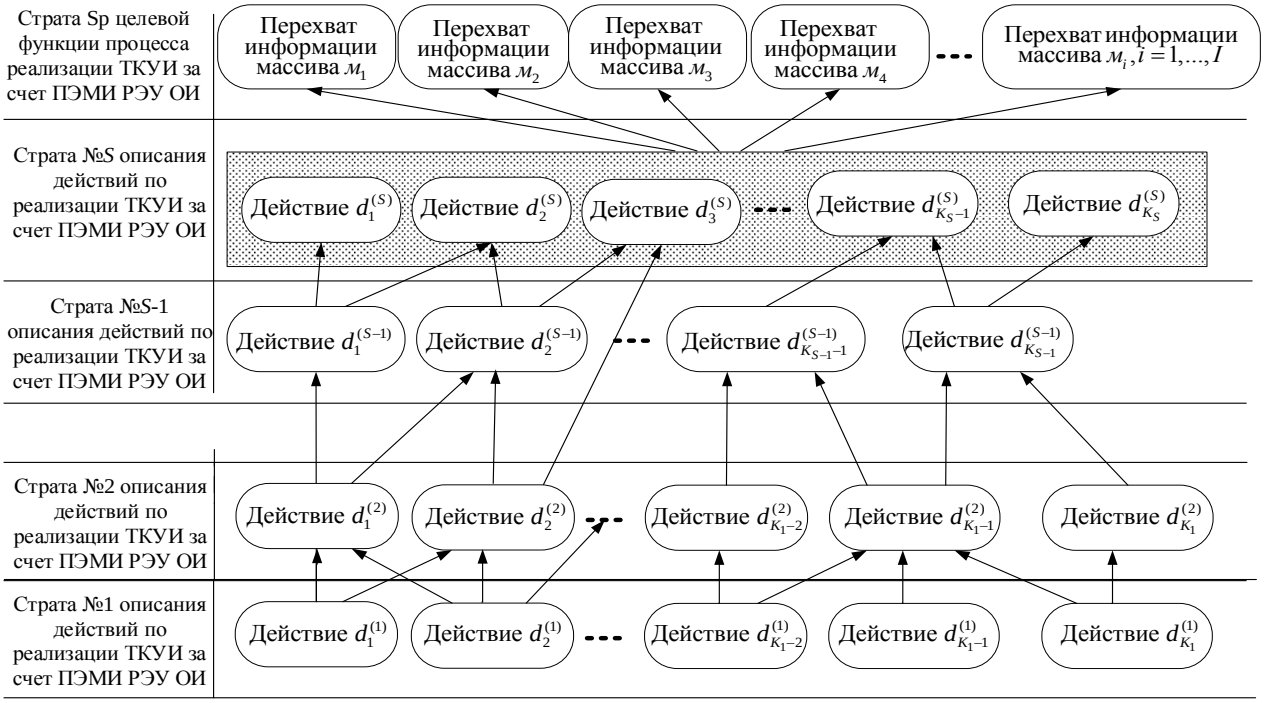

Рис. 4. Иллюстрация стратифицированного описания процесса реализации угроз утечки информации за счет побочных электромагнитных излучений радиоэлектронных устройств объекта информатизации

Страта (S–1) соответствует выполненному условию (1). На страте S определяется выполнение совокупности условий (например, условий (1) и (2)) для реализации процесса перехвата информации. На заключительной страте осуществляется проверка выполнения требований к свойствам перехваченной информации (условие (3)) того или иного вида (массива $м_i$, i=1, 2, …, I) и ее отображение ПИ. Из рисунка видно, что для реализации процесса перехвата информации того или иного вида, например речевой информации в аналоговой форме представления с диапазоном воспроизводимых частот, соответствующим каналу тональной частоты ($\Delta f = 0{,}3-3{,}4$ кГц), возможно выполнение различных последовательностей действий на стратах описания этого процесса.

Совокупности действий определяют условия реализации процесса перехвата информации различного вида. Например, к таким совокупностям действий могут относиться:

$$d_1^{(1)} \to d_1^{(2)} \to d_1^{(S-1)} \to d_1^{(S)} \to d_{м_1}^{(Sp)};$$

$$(d_2^{(1)} \to d_1^{(2)} \to d_2^{(S-1)}) \& (d_2^{(1)} \to d_2^{(2)} \to d_2^{(S-1)}) \to d_2^{(S)} \to d_{м_2}^{(Sp)};$$

$$(d_2^{(1)} \to d_2^{(2)}) \& (d_2^{(1)} \to d_1^{(2)} \to d_2^{(S-1)}) \to d_3^{(S)} \to d_{м_3}^{(Sp)} \ldots;$$

$$\left(d_{K_1-2}^{(1)} \to d_{K_2-2}^{(2)}\right) \& \left(d_{K_1-2}^{(1)} \to d_{K_2-1}^{(2)}\right) \to d_{K_{S-1}-1}^{(S-1)} \to$$
$$\to d_{K_S-1}^{(S)} \to d_{м_4}^{(Sp)};$$

$$\left(d_{K_1}^{(1)} \to d_{K_2-1}^{(2)} \to d_{K_{S-1}}^{(S-1)}\right) \& \left(d_{K_1}^{(1)} \to d_{K_2}^{(2)} \to d_{K_{S-1}}^{(S-1)}\right) \to$$
$$\to d_{K_S}^{(S)} \to d_{м_5}^{(Sp)}.$$

Некоторые из таких совокупностей представляют композицию действий, выполняемых параллельно и независимо одно от другого. Это усложняет оценку общего времени реализации угрозы рассматриваемого типа.

В качестве примера можно привести графическую интерпретацию параллельно выполняемых действий по обеспечению условий (1) и (2), представленную на рис. 3.

На рис. 4 эти условия могут быть иллюстрированы в виде совокупности действий:

$$d_2^{(1)} \to (d_2^{(2)} \to d_2^{(S-1)}) \& (d_2^{(2)} \to d_3^{(S)}) \to d_3^{(S)} \to d_{м_i}^{(Sp)} \ldots.$$

Таким образом, для каждого варианта описания процесса реализации ТКУИ рассматриваемого типа может быть определена композиция возможных совокупностей действий, выполненных на предыдущих стратах описания этого процесса и направленных на создание условий для его реализации.

Формально функциональная модель процесса реализации ТКУИ за счет ПЭМИ РЭУ ОИ может быть представлена как совокупность трех множеств [24]

$$\mathbf{\Phi}_u = \left\{\mathbf{D}_u, \mathbf{M}(\mathbf{D}_u), \mathbf{Y}(\mathbf{D}_u)\right\}, u = \overline{1,U}, \qquad (15)$$

где $\mathbf{D}_u$ – множество действий $\mathbf{d}_u^{(k)} \in \mathbf{D}_u, k = \overline{1,K}$, выполняемых для реализации u-го варианта ТКУИ; K – мощность множества $\mathbf{D}_u$; $\mathbf{M}(\mathbf{D}_u)$ – матрица взаимосвязей действий $\mathbf{d}_u^{(k)}$ в порядке их выполнения; $\mathbf{Y}(\mathbf{D}_u)$ – совокупность условий для выполнения действий $\mathbf{d}_u^{(k)} \in \mathbf{D}_u$, при которых реализация u-го варианта ТКУИ возможна.

С использованием такого представления могут быть разработаны функциональные модели процессов реализации ТКУИ за счет ПЭМИ РЭУ ОИ, включающие совокупности подлежащих выполнению действий по обеспечению согласования разнородных характеристик сигналов ПЭМИ с соответствующими характеристиками РРП, учитывающие взаимосвязи этих действий, условия их выполнения, а также примерные оценки времени выполнения каждого действия.

В качестве примера на рис. 5 приведена функциональная модель варианта последовательно выполняемых нарушителем действий в процессе реализации перехвата речевой информации, циркулирующей в выделенном помещении, предназначенном для проведения мероприятий с применением ТС звукоусиления и связи.

В левом столбце матрицы $\mathbf{M}(\mathbf{D}_{1.1})$ взаимосвязей на этом рисунке указаны номера выполняемых действий, в верхней строке – номера последующих действий. Условия выполнения этих действий не определены: множество $\mathbf{Y}(\mathbf{D}_{1.1})$ – пустое.

На рис. 6 представлена функциональная модель, соответствующая параллельному выполнению действий по реализации процесса ПрПИ.

Обозначение и описание действий, выполняемых в ходе моделируемого варианта процесса реализации угрозы – приведены в табл. 2.

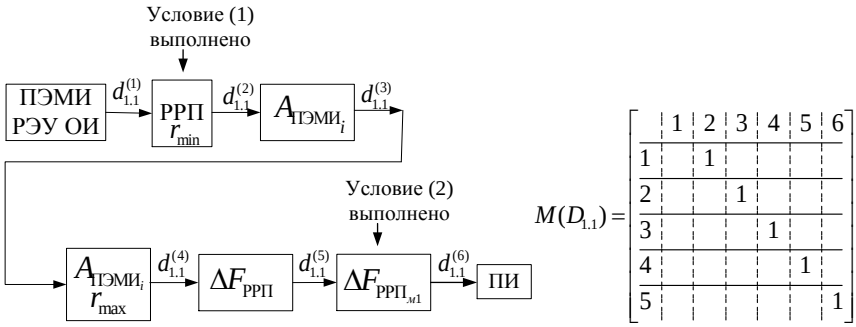

Рис. 5. Функциональная модель варианта последовательно выполняемых нарушителем действий в процессе реализации перехвата речевой информации, циркулирующей в выделенном помещении. Без мер защиты

Таблица 2

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

Наименование угрозы	Содержание действий, выполняемых при реализации угрозы	Обозначение действий	Время выполнения действий, мин
	Вариант № 1		
Реализация процесса перехвата речевой информации, циркулирующей в выделенном помещении, оборудованном средствами звукоусиления и связи	Нарушитель выбирает место применения РРП ($r = r_{\min}$), при котором обеспечиваются условия скрытности	$d_{1.1}^{(1)}$	8–12
	Выполнено сканирование частотного диапазона при условии, соответствующем формуле (1)	$d_{1.1}^{(2)}$	3–5
	С использованием направленной антенны определено направление максимального уровня излучения ПЭМИ	$d_{1.1}^{(3)}$	5–7
	Скорректировано расстояние ($r = r_{\max}$) применения РРП, при котором обеспечивается скрытность его применения	$d_{1.1}^{(4)}$	8–12
	Выбран режим работы, обеспечивающий соответствие характеристик РРП характеристикам перехватываемого сигнала ПЭМИ с целью выполнения условия, соответствующего формуле (2)	$d_{1.1}^{(5)}$	3–5
	Выполнена проверка свойств перехваченной информации в соответствии с условиями (11)–(13)	$d_{1.1}^{(6)}$	5–10

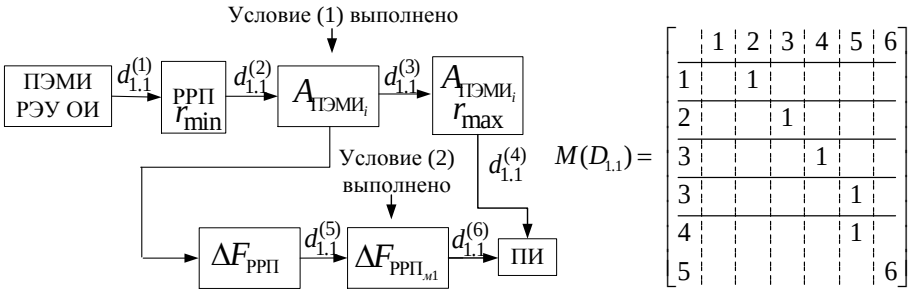

Рис. 6. Функциональная модель варианта параллельно выполняемых нарушителем действий в процессе реализации перехвата речевой информации, циркулирующей в выделенном помещении. Без мер защиты

Сравнивая данные табл. 1 и 2, определим степень соответствия свойств перехваченной информации требованиям нарушителя для функциональной схемы на рис. 6:

$$\tau_{ИПр} \approx 35 мин;\ \tau_{ПрПИ} \approx 34 мин;\ \tau^{*}_{ИПр} \approx 1 мин.$$

Процесс ПрПИ в рассматриваемых условиях не реализован.

При параллельном выполнении нарушителем некоторых действий, направленных на обеспечение условий (1) и (2), время реализации процесса ПрПИ сокращается на 4 минуты, что соответствует $\tau^{*}_{ИПр} \approx 5 мин$, и перехват информации нарушителем можно считать реализованным успешно.

Заключение

Функциональное моделирование используется для предварительной формализации исследуемых процессов. Однако представленные функциональные модели по аналогии с [25, 26] могут служить основой для разработки с использованием аппарата сетей Петри-Маркова аналитических моделей динамики реализации угроз утечки информации по техническим каналам за счет ПЭМИ РЭУ ОИ, учитывающих вероятностно-временные характеристики действий, выполняемых последовательно-параллельно, и при наличии определенных логических условий, адекватно отражающих процессы реализации угрозы для конкретного ОИ и позволяющих получить аналитические соотношения для расчета показателей защищенности информации от утечки как в условиях применения мер защиты, так и без применения этих мер.

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/document/gost-r-51275-2006.

2. Авсентьев О.С. Формирование обобщенного показателя ценности информации в каналах связи / О.С. Авсентьев, А.О. Авсентьев // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 55–63.

3. 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.

4. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утв. приказом Гостехкомиссии России от 30.08.2002 № 282 [Электронный ресурс]. – Режим доступа: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm, свободный (дата обращения: 25.02.2019).

5. Авсентьев О.С. Моделирование и оптимизация процессов передачи и защиты информации в каналах связи / О.С. Авсентьев, В.В. Меньших, А.О. Авсентьев // Специальная техника. – 2015. – № 5. – С. 47–50.

6. 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.

7. 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.

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

9. 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 института МВД России. – 2017. – № 2. – С. 125–135.

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

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

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

13. Никольский Б.А. Основы радиотехнических систем [Электронный ресурс]. – Электрон. текстовые и граф. дан. (3,612 Мбайт). – Самара, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т), 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. 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.

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

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

18. 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.

19. Смирнов В.В. Устройства СВЧ и антенны: учеб. пособие / В.В. Смирнов, В.П. Смолин. – СПб.: Балт. гос. техн. ун-т., 2012. – 188 с.

20. Тихонов В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов. – М.: Сов. радио, 1977. – 488 с.

21. Сильверстов Д.С. Полумарковские процессы с дискретным множеством состояний. – М.: Сов. радио, 1980. – 272 с.

22. Игнатьев В.М. Сети Петри–Маркова / В.М. Игнатьев, Е.В. Ларкин. – Тула: ТулГТУ, 1994.

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

24. Авсентьев О.С. Функциональные модели процессов реализации угроз электронному документообороту /

О.С. Авсентьев, А.О. Авсентьев, И.О. Рубцова // Вестник ВИ МВД. – 2019. – № 4. – С. 40–50.

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

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

Авсентьев Олег Сергеевич
Д-р техн. наук, проф. каф. информационной безопасности
Воронежского института МВД России
Патриотов пр-т, 53, г. Воронеж, Россия, 394065
Тел.: +7 (473-2) 00-52-44; +7-903-655-55-14
Эл. почта: osaos@mail.ru

Кругов Артем Геннадьевич
Главный специалист Центра
информационных технологий, связи и защиты
информации УМВД России по Тверской обл.
Мира пл., д. 1/70, г. Тверь, Россия, 170100
Тел.: +7 (482-2) 32-93-93; +7-920-697-18-68
Эл. почта: krtemik@gmail.com

Шелупанова Полина Александровна
Канд. экон. наук, доцент каф. безопасности
информационных систем ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-39-39
Эл. почта: pi6-mne@yandex.ru

Avsentev O.S., Krugov A.G., Shelupanova P.A.

Functional models of processes for implementing information leakage threats due to side electromagnetic radiation of informatization objects

The approach to constructing functional models of the processes of implementing threats of information leakage through technical channels due to the side electromagnetic radiation of electronic devices of informatization objects is considered, based on the stratified representation of such processes, which reflects the relationship between the actions of the intruder carried out on different description strata in the form of a set of actions corresponding to each of the possible options for the implementation of processes of the type in question.

Keywords: technical channel of information leakage, incident electromagnetic radiation, functional model, information transmission path, signal characteristics, object of informatization, electronic device.
doi: 10.21293/1818-0442-2020-23-1-29-39

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. 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.).

3. 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.).

4. «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.).

5. Avsentev O.S., Menshikh V.V., Avsentev A.O. *Modelirovaniye i optimizatsiya protsessov peredachi i zashchity informatsii v kanalakh svyazi* [Modeling and optimization of information transmission and protection processes in communications channels]. *Special Technique*, 2015, no. 5, pp. 47–50 (in Russ.).

6. 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.).

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

8. 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.).

9. 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.).

10. 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.).

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

12. 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.).

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. Glushkov V.A., Dormidontov A.V. Nesterenko A.G. *Teoriya elektricheskoy svyazi: uchebnoye posobiye* [Theory of electrical communication, tutorial, general. ed. K.K. Vasiliev]. Ulyanovsk, UlSTU, 2008. 452 p. (in Russ.).

15. 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.).

16. 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.).

17. 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.).

18. 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.).

19. Smirnov V.V., Smolin V.P. *Ustroystva SVCH i antenny: uchebnoye posobiye* [Microwave devices and antennas: study guide]. SPb., Balt. state tech. un-t, 2012, 188 p. (in Russ.).

20. Tikhonov V.I., Mironov M.A. *Markovskiye protsessy* [Markov processes. M., Sov. radio, 1977, 488 p. (in Russ.).

21. Silverstov D.S. *Polumarkovskiye protsessy s diskretnym mnozhestvom sostoyaniy* [Semi-Markov processes with a discrete set of states]. M., Sov. radio, 1980, 272 p. (in Russ.).

22. Ignatiev V.M. *Seti Petri–Markova* [Petri Markov networks]. Tula, TulGTU, 1994.

23. 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.).

24. Avsentev O.S., Avsentev A.O., Rubtsova I.O. *Funktsional'nyye modeli protsessov realizatsii ugroz elektronnomu dokumentooborotu* [Functional models of processes for implementing threats to electronic document management]. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2019, no. 4, pp. 40–50 (in Russ.).

25. 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-o/D, Publishing House SKNTs VSh, 2006, 274 p. (in Russ.).

26. Avsentev O.S., Rubtsova I.O., Yazov Y.K. *K voprosu ob otsenke effektivnosti zashchity informatsii v sistemakh elektronnogo dokumentooborota* [On the Evaluation of the Effectiveness Information Protection in Electronic Document Management Systems]. *Cybersecurity Iss.* 2019, no. 1(29), pp. 25–34 (in Russ.).

Oleg S. Avsentev
Doctor of Engineering Sciences, Professor,
Department of Information Security,
Voronezh Institute of the Ministry of Internal Affairs of Russia
53, Patriotov pr., Voronezh, Russia, 394065
Phone: +7 (473-2) 00-52-44; +7-903-655-55-14
E-mail: osaos@mail.ru

Artem G. Krugov
Leading specialist, Center of Information Technology,
Communications and Information Protection.
Ministry of Internal Affairs of Russia in the Tver Region
1/70, Mira Sq., Tver, Russia, 170100
Phone: +7 (482-2) 32-93-93; +7-920-697-18-68
E-mail: krtemik@gmail.com

Polina A. Shelupanova
Candidate in Economics, Associate Professor,
Chair of Information Systems Security, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-(382-2) 41-39-39
Email: pi6-mne@yandex.ru