Сухомлина Кристина Андреевна
Воронежский институт МВД России

ОБЩЕЕ ОПИСАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ ПО ОБРАБОТКЕ И ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

GENERAL DESCRIPTION OF INFORMATION PROCESSES ON PROCESSING AND PROTECTION OF SPEECH INFORMATION ON THE OBJECTS OF INFORMATIZATION INTERNAL AFFAIRS BODIES

Предложен подход к описанию реализации информационных процессов с использованием речевой информации на объектах информатизации органов внутренних дел, учитывающий особенности формирования, распространения и использования такого рода информации в деятельности органов внутренних дел. Рассмотрены сценарии динамики параллельно реализуемых процессов обработки этой информации и угроз нарушения ее безопасности нарушителем. Предлагается в интересах количественной оценки защищенности речевой информации в этих условиях применять аппарат составных сетей Петри-Маркова.

An approach to the description of the implementation of information processes using speech information on the information objects of internal affairs bodies, taking into account the peculiarities of the formation, distribution and use of this kind of information in the activities of internal affairs bodies is proposed. Scenarios of dynamics of parallel processes of processing of this information and threats of violation of its security by an intruder are considered. It is proposed in the interests of quantitative assessment of security of speech information in these conditions to apply the apparatus of compound Petri-Markov networks.

1. Введение. При реализации деятельности, осуществляемой по различным направлениям «…для защиты жизни, здоровья, прав и свобод граждан Российской Федерации, …, охраны общественного порядка, собственности и для обеспечения общественной безопасности…», органы внутренних дел (ОВД) используют достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру [1]. При этом совокупность информационных ресурсов, средств и систем обработки информации, 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, составляют объекты информатизации (ОИ) [2].

Информационные ресурсы ОИ, включающие совокупность данных, организованных для получения достоверной информации в самых разных областях знаний и практической деятельности, формируются путем реализации информационных процессов (ИПр) – процессов сбора, обработки, накопления, хранения, поиска и распространения (далее, – обработки) информации.

Одним из требований к реализации ИПр в деятельности ОВД является оперативность их реализации, характеризующая незамедлительность (своевременность) оказания помощи каждому, кто нуждается в её защите от преступных и иных противоправных посягательств [1]. При этом основной формой представления обрабатываемой информации является речевая информация (РИ), в качестве материального носителя которой используются акустические колебания (сигналы) упругой среды (воздушной, жидкостной или твердой).

Реализация ИПр с использованием речевой формы представления информации имеет ряд положительных качеств: своевременность их реализации; аутентичность источника сведений (идентификацию), а следовательно, и их подлинность по содержанию; защищенность этих сведений (при обеспечении некоторых условий) от подмены и имитации.

Однако использование акустических колебаний в качестве материального носителя РИ является объективным фактором, воздействующим на безопасность информации [2], и, в первую очередь, фактором, обусловливающим возможность реализации угроз нарушения ее конфиденциальности. Это связано с особенностями формирования, распространения и использования РИ, с одной стороны, легитимными пользователями, с другой стороны, пользователями, выступающими в качестве источников такого рода угроз. Особенности формирования РИ связаны, во-первых, с энергетическими и частотными характеристиками ее источника, во-вторых, с временными характеристиками, характеризующими динамику реализации ИПр, в-третьих, с использованием в качестве среды распространения акустических колебаний акустического поля, воздействующего на элементы интерьера помещений и структурные элементы (в том числе радиоэлектронные устройства) ИС ОИ, что позволяет их рассматривать в качестве вторичных источников информации, с одной стороны, в структуре технических средств и систем на ОИ (основных технических средств и систем (ОТСС) [3]), с другой стороны, в качестве датчиков информации (ДИ) в составе вспомогательных технических средств и систем (ВТСС), которые могут использоваться нарушителем для формирования различного рода технических каналов утечки информации такого рода [3]. Условия распространения определяются свойствами сред распространения. Особенности использования РИ в деятельности ОВД и при реализации нарушителем процесса ее перехвата (ПрПИ) зависят от возможностей пользователей(легитимных и нелегитимных соответственно) по приему

акустических колебаний и адекватному восприятию содержащихся в них сведений. При этом считается, что перехват РИ возможен тогда, когда она содержится в принимаемых акустических колебаниях и представляет интерес для нарушителя. Указанные особенности в рамках ИПр взаимосвязаны. Однако современным методическим обеспечением защиты РИ от утечки по техническим каналам [3] указанные взаимосвязи не учитываются, а применяемые в настоящее время для реализации мер защиты расчетно-измерительные методики учитывают только энергетические характеристики акустических (речевых) сигналов, содержащих РИ, и не учитывают, во-первых, динамику реализации ИПр и ПрПИ и, во-вторых, взаимосвязи этих процессов. Учет указанной динамики может не только существенно повлиять на защищенность РИ на ОИ от утечки, но и изменить требования по защите.

Указанные обстоятельства свидетельствуют об актуальности данной работы, посвященной исследованию вопросов разработки описательных моделей процессов обработки и защиты РИ на ОИ ОВД различного назначения.

2. Описание условий формирования и использования речевой информации на объектах информатизации ОВД. Условия формирования и использования РИ в деятельности ОВД в существенной степени зависят от назначения и структурно-функциональных характеристик ОИ.

В системе ОВД России к ОИ могут быть отнесены переговорные кабины $ОИ_1$, служебные кабинеты сотрудников $ОИ_2$, помещения информационно-вычислительных центров $ОИ_3$, ситуационные центры $ОИ_4$ и др.

В качестве примера рассмотрим условия формирования и использования РИ в выделенных помещениях (ВП) [3], относящихся к $ОИ_1$ и предназначенных для реализации ИПр путем обмена РИ, содержащей сведения ограниченного доступа, между двумя (или более) участниками без использования технических средств, относящихся к ОТСС. Однако в составе такого рода ВП, как правило, имеются ВТСС жизнеобеспечения (систем освещения, вентиляции, охранно-пожарной сигнализации и др.). Структурно-логическое представление такого рода ВП приведено на рис.1.

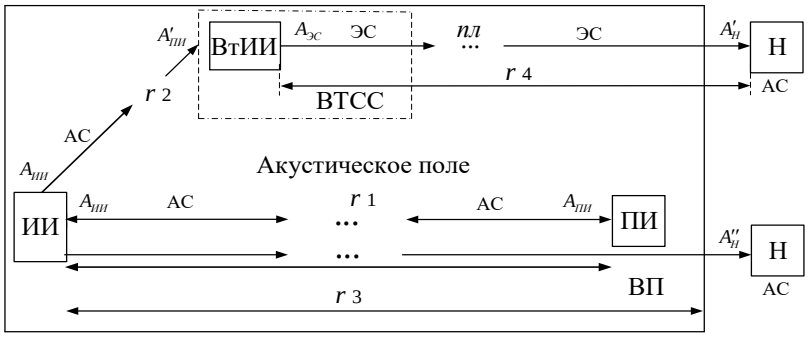

Рис.1 Структурно-логическое представление выделенного помещения

Источником и получателем (ИИ и ПИ, соответственно) РИ являются участники переговоров. Переговоры, как правило, осуществляются в режиме диалога (каждый из участников может выступать в качестве ИИ или ПИ). Уровень (амплитуда) акустических (речевых) сигналов (АС), используемых для реализации ИПр ($A_{ИИ}$ и $A_{ПИ}$ на выходе ИИ и на входе ПИ, соответственно), соответствует размерам ВП, определяющим расстояния r_1 между участниками переговоров. При этом значения $A_{ИИ}$ и $A_{ПИ}$ связаны соотношением:

$$A_{ПИ} = k_o(r_1) \cdot A_{ИИ}, \quad (1)$$

где $A_{ИИ}$ и $A_{ПИ}$ амплитуды АС на выходе ИИ и на входе ПИ, соответственно;

$k_o(r_1)$ – коэффициент ослабления воздушной среды;

r_1 – расстояние между участниками переговоров.

В качестве среды распространения этих сигналов рассматривается воздух, а возникающее на выходе ИИ акустическое поле (АП) имеет круговую диаграмму направленности излучения. АС через АП воздействует на элементы интерьера ВП, на его ограждающие конструкции(ОК)(пол, потолок, стены, оконные рамы и стекла и др.). При недостаточном уровне звукоизоляции ВП АС могут быть приняты нарушителем за пределами ВП с уровнем A''_H:

$$A''_H = A_{ИИ} \cdot k_o(r_3) \cdot k_{ОК}, \quad (2)$$

где $k_o(r_3)$ – ослабление АС на расстоянии r_3 от ИИ до ограждающей конструкции;

$k_{ОК}$ – коэффициент ослабления ОК.

Элементы ВТСС располагаются в ВП в пределах воздействия АП. Уровень акустического сигнала АС, воздействующего на структурный элемент ВТСС, обладающий свойствами акусто-электрического преобразующего устройства и выступающего в качестве вторичного источника информации (ВтИИ), определяется в соответствии с соотношением:

$$A'_{ПИ} = k_o(r_2) \cdot A_{ИИ}. \quad (3)$$

На выходе ВтИИ формируется отклик в виде колебаний электрического тока – электрический сигнал (ЭС), содержащий передаваемое речевое сообщение. По проводным линиям (*пл*) ВТСС, выходящим за пределы ВП, используемым в качестве проводной среды распространения, ЭС, содержащий РИ может быть перехвачен нарушителем (Н) за пределами ВП путем подключения к этим линиям специального разведывательного приемника. Уровень ЭС на входе этого приемника определяется соотношением:

$$A'_H = A_{ЭС} \cdot k_{пл}(r_4), \quad (4)$$

где $k_{пл}(r_4)$ – ослабление ЭС на расстоянии r_4 от ВтИИ до места подключения разведывательного приемника нарушителя к проводной линии ВТСС;

$k_{пл}$ – коэффициент ослабления ОК.

Речевой сигнал(РС) представляет собой совокупность множества частотных составляющих в диапазоне от 20 Гц до 20000 Гц. При этом основная энергия такого сигнала сосредоточена в области частот от 300 до 4000 Гц. Такая полоса частот считается достаточной для обеспечения приемлемой для ПИ разборчивости речи с возможностью идентификации говорящего [4]. Зависимость между энергетическими и частотными параметрами РС имеет сложный характер [5]. Если в пределах ВП эта зависимость практически не проявляется, то при оценке возможностей нарушителя по перехвату РИ за пределами ВП зависимость коэффициента ослабления ЭС в проводных линиях или АС при его прохождении через ОК учитывается, в том числе и существующим методическим обеспечением. Однако, как было отмечено ранее, перехват РИ считается успешным в случае, когда эта информация представляет интерес для нарушителя и может им использоваться для нарушения деятельности ОВД. Данное обстоятельство характеризует динамику реализации ИПр на ОИ и динамику реализации процессов ее перехвата нарушителем и обусловливает необходимость учета этой динамики при оценке защищенности РИ от утечки по техническим каналам.

3. Описание сценариев реализации информационных процессов с использованием речевой информации и процессов реализации угроз в отношении этой информации на объектах информатизации. Переговоры между их участниками на $ОИ_1$ осуществляются в режиме диалога. При этом источники информации и ее получатели на рисунке 1 меняются местами. В результате изменяется расстояния r_2 и r_3 (рисунок 1), что приводит к изменениям условий перехвата информации как за пределами ОК (за счет изменений коэффициента $k_o(r_3)$ в (2)), так и по проводным линиям ВТСС, выходящим за пределы $ОИ_1$ (за счет изменений коэффициента $k_o(r_2)$ в (3)). Кроме того, изменения мест расположения ИИ и ПИ в режиме диалога имеют случайный характер. Случайными также являются и временные характеристики фрагментов речи (начало, окончание, продолжительность) различных участников переговоров. При этом содержание не каждого фрагмента речи и не каждого участника переговоров может представлять интерес для нарушителя. Иллюстрация динамики реализации ИПр с использованием РИ на $ОИ_1$ приведена на рисунке 2.

На рисунке 2 используются следующие обозначения:

t_0 – время начала рабочего дня; t_1 – время начала реализации ИПр(переговоров); t_2 – время окончания ИПр(переговоров); $\tau^1_{ИПр1}$, …, $\tau^I_{ИПр1}$ – продолжительности реализации фрагментов речи первого участника

переговоров; $\tau_{ИПр1}$ – продолжительность всего процесса ИПр1; μ_{P1}^{1} – μ_{P1}^{I-1} – продолжительности пауз между фрагментами речи первого участника переговоров; $\tau_{ИПр2}^{1}$, …, $\tau_{ИПр2}^{I}$ – продолжительности реализации фрагментов речи второго участника переговоров; $\tau_{ИПр2}$ – продолжительность всего процесса ИПр2; μ_{P2}^{1} – μ_{P2}^{I} – продолжительности пауз между фрагментами речи второго участника переговоров; μ_{p1-2}^{1} – μ_{P1-2}^{I} – продолжительности пауз между фрагментами речей участников переговоров.

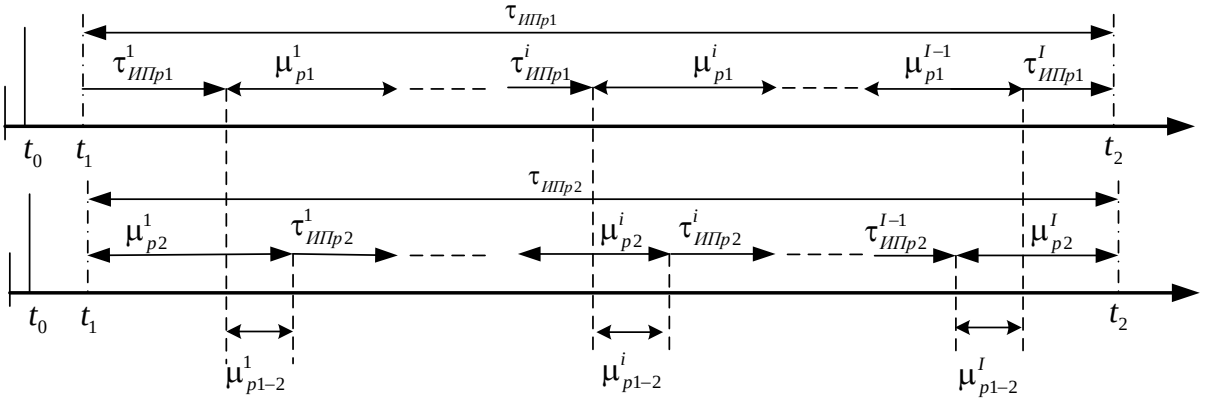

Рисунок 2. Иллюстрация сценария реализации ИПр с использованием РИ на $ОИ_1$

В этих условиях возможны различные сценарии реализации нарушителем процесса ПрПИ:

– нарушитель постоянно находится в зоне возможной реализации ПрПИ путем подключения приемника перехвата к проводным линиям ВТСС, выходящим за пределы $ОИ_1$ или съема РИ с ОК объекта;

– нарушитель постоянно находится в зоне возможной реализации ПрПИ.

В первом случае успех реализации перехвата РИ на $ОИ_1$ определяется лишь динамикой реализации ИПр.

Во втором случае динамика успеха реализации перехвата РИ на $ОИ_1$ определяется не только условиями реализации переговоров, но и возможностями проникновения нарушителя в зону возможной реализации ПрПИ, а также наличием в его распоряжении приемника с необходимыми характеристиками (подключение к проводным линиям ВТСС или наличие в составе приемника датчика для съема РИ с ОК ВП). Очевидно, что временные характеристики реализации нарушителем процесса ПрПИ также случайны. Указанные обстоятельства обусловливают сложность получения адекватных оценок защищенности РИ от утечки по техническим каналам. Применение для такой оценки существующего методического обеспечения, основанного, во-первых, на экспертных методах и, во-вторых, на расчетно-измерительных

методиках, учитывающих только энергетические характеристики РС, как правило, дает завышенные результаты оценки угроз утечки РИ в рассматриваемых условиях. Применение методов моделирования на основе имитационных и функциональных моделей, а также получение численных оценок с использованием моделей на основе Марковских или полумарковских процессов не позволяет учитывать динамику реализации параллельно реализуемых и взаимосвязанных процессов ИПр и ПрПИ. Кроме того, применение такого рода моделей не позволяет оценить эффективность систем защиты РИ в рассматриваемых условиях, а также возможности применения мер защиты адаптированных к условиям динамики исследуемых процессов [6].

4. Процесс перехвата информации по техническим каналам на этапе создания объекта информатизации.

В связи с тем что процессы ИПр, ПрПИ и ПрЗИ взаимосвязаны, при создании каждого конкретного ОИ необходимо разрабатывать свои модели с учетом формы представления обрабатываемой информации и ее материальных носителей, вида и формы представления формируемых документов, условий их разработки и хранения, а также временных характеристик реализации этих процессов.

В частности, при разработке моделей ПрПИ необходимо учитывать следующее:

– временные характеристики реализации ИПр, то есть время, в течение которого осуществляется процесс и возможна утечка конфиденциальной информации; для нарушителя это время неизвестно, а ПрПИ является случайным во времени процессом;

– ИПр может включать несколько последовательно-параллельно реализуемых в интересах разработки различных документов частных процессов ИПр, каждый из которых, в свою очередь, может включать несколько парциальных процессов;

– не вся информация, обрабатываемая в ходе реализации ИПр, содержит конфиденциальные сведения, представляющие интерес для нарушителя; времена возникновения фрагментов, содержащих такие сведения, и их длительность являются случайными;

– с учетом обеспечения скрытности ПрПИ время его реализации нарушителем ограниченно и случайно, поскольку он может быть обнаружен средствами СКУД ИСС (внутренний нарушитель, проникший в помещение создаваемого ОИ) или за счет реализации адаптивных мер защиты на территории, прилегающей к помещениям организации (внешний нарушитель);

– в ходе реализации ПРПИ нарушитель выполняет ряд действий, связанных, например, с установкой в помещениях организации закладочных устройств (внутренний нарушитель), или с обеспечением, во-первых, выбора ТСП, соответствующего виду перехватываемой информации, во-вторых, скрытности его применения при формировании ТКУИ с учетом характеристик территории, прилегающей к помещениям организации [8, 10]; время

выполнения указанных действий является случайной величиной;

– для обнаружения и пресечения попыток нарушителя по перехвату информации, содержащейся в документах, формируемых в процессе реализации ИПр, или документа (документов); в целом по завершении этого процесса в интересах защиты информации от утечки могут быть применены как превентивно установленные средства ИТУ и СКУД в составе ИСС, так и организационно-технические меры, адаптированные к выполнению нарушителем действий по реализации процесса ПрПИ.

При необходимости оценки возможности перехвата нарушителем информации, обрабатываемой в интересах разработки документов, в условиях применения мер защиты в ходе последовательно-параллельной реализации фрагментов ИПр необходимо учитывать вероятностно-временные характеристики процессов ПрЗИ и взаимосвязь как этих процессов, так и применяемых мер между собой. Для учета этих взаимосвязей вводятся логические условия, определяющие порядок применения мер защиты.

5. Заключение. Представленные описания сценариев параллельно реализуемых и взаимосвязанных процессов обработки РИ на ОИ ОВД, действий нарушителей по реализации угроз безопасности в отношении этой информации, могут использоваться для формирования функциональных, а на их основе аналитических моделей такого рода процессов в целях получения численных оценок защищенности информации. Поскольку действия нарушителя по реализации УБИ и действия сотрудников подразделения ОВД, участвующих в реализации процессов ИПр могут выполняться как последовательно, так и параллельно в зависимости от различного рода условий их выполнения, для разработки таких моделей целесообразно использовать аппарат сетей Петри-Маркова [6–8]. Разработка таких моделей является предметом дальнейших исследований авторов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ЛИТЕРАТУРЫ

1. О полиции : Федеральный закон от 7 февраля 2011 г. № 3–ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 7. – Ст. 900.

2. ГОСТ Р 51275-2006: Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Утвержден и введен в действие ром Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374–ст.

3. Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – Москва : Гостехкомиссия России, 2002. – 80 с.

4. Бондарко Л. В. Основы общей фонетики : учебное пособие / Л. В. Бондаренко, Л. А. Вербицкая, М. В. Гордина. – Санкт-Петербург : Изд-во Санкт-Петербурского университета, 1991. – 152 с.

5. Л. Фланаган Джеймс. Анализ, синтез и восприятие речи. Перевод с английского под редакцией А. А. Пирогова / Джеймс Л. Фланаган. – Москва : Издательство «Связь», 1968. – 396 с.

6. Simulation of processes to protect information of informatization objects against leakage through technical channels using an apparatus of Petri–Markov nets / O. S. Avsentiev, A. O. Avsentiev, A.G. Krugov, Yu. K. Yazov. //Bulletin of the South Ural StateUniversity. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS), 2021, vol. 14, no. 4, pp. 46–62.

7. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри–Маркова / О. С. Авсентьев, А. О. Авсентьев, Ю. К. Язов, И. О. Рубцова // Труды СПИИРАН. 2019. Том 18, № 6. С. 1269–1300

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