Кругов Артём Геннадьевич,
начальник отдела
ФГКУ «УВО ВНГ России
по Тверской области»

МОДЕЛИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОТ УТЕЧКИ ЗА СЧЕТ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ

MODELS FOR ASSESSING INFORMATION SECURITY FROM LEAKAGE DUE TO SPURIOUS ELECTROMAGNETIC RADIATIONS AT INFORMATIZATION OBJECTS OF THE FEDERAL NATIONAL GUARD TROOPS SERVICE

В работе представлена модель оценки защищенности информации от утечки за счет побочных электромагнитных излучений на объектах информатизации федеральной службы войск национальной гвардии.

The paper presents a model for assessing the security of information from leakage due to side electromagnetic radiation at the informatization facilities of the Federal Service of the National Guard troops.

Деятельность федеральной службы войск национальной гвардии (далее ФСВНГ), в интересах обеспечения которой создаются объекты информатизации, осуществляется по направлениям, отличающимся по целям, задачам, составу участников реализации (охрана общественного порядка, собственности, обеспечение общественной безопасности, участие в борьбе с терроризмом и экстремизмом и др.). При этом содержание информации, циркулирующей на этих объектах представляет интерес для различных заинтересованных сторон (нарушителей):

– спецслужб иностранных государств;

– криминальных структур;

– организаций и отдельных физических лиц, имеющих противоправные или иные цели.

В связи с этим последствия, то есть ущерб, причиняемый ФСВНГ, а следовательно, и гражданам, общественным или государственным организациям, в результате утечки информации, используемой в интересах деятельности по каждому из этих направлений, также отличаются.

Информация, используемая в интересах обеспечения деятельности

ФСВНГ обрабатывается на объектах, которые в этих условиях являются объектами информатизации. При этом к объектам информатизации относятся различные помещения (служебные кабинеты, актовые, конференц-залы и т.д.), а также автоматизированные информационные системы на основе средств вычислительной техники.

Поскольку деятельность ФСВНГ по указанным направлениям, как правило, носит конфиденциальный характер, то информация, не содержащая сведений, составляющих государственную тайну, циркулирующая на объектах информатизации рассматриваемого типа, является объектом защиты, в том числе от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений структурных элементов объекта (далее ПЭМИ). К таким структурным элементам относятся различные технические средства и системы, их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации – основные технические средства и системы (ОТСС), а также различного назначения вспомогательные технические средства и системы (ВТСС). При этом объектами защиты являются также и охраняемая территория, здание (сооружение), а также помещения, в которых располагаются указанные структурные элементы.

Особенность объектов информатизации ФСВНГ, а особенно ее территориальных органов и подчиненных им подразделений, состоит в том, что до настоящего времени здания таких подразделений располагаются в условиях городской застройки в центральных районах населенных пунктов, территория в большинстве случаев охраняется только в рамках ограждающих конструкций этих зданий, а помещения объектов информатизации размещаются без учета конфигурации этой территории, а также территории, прилегающей к самим зданиям. Это позволяет различным гражданам находиться и передвигаться в пешем порядке или на машинах на территории, прилегающей к зданию, в непосредственной близости от их объектов информатизации, что в существенной степени затрудняет организацию и обеспечение контроля за их действиями, которые могут быть направлены на реализацию угроз утечки информации, циркулирующей на объектах. Протяженность этой территории, например, ширина улиц, а следовательно, и расстояние до противоположных зданий часто не превышает 10 метров. Между тем дальность обнаружения радиоизлучений, например, широко распространенных персональных ЭВМ зарубежного производства с возможностью отображения содержащейся в них информации значительно превышают эти расстояния. Перехват более помехоустойчивых узкополосных ПЭМИ, функционально присущих работе различного рода радиоэлектронных устройств и содержащих, например, речевую информацию, возможен на еще больших расстояниях[1].

В соответствии с существующим методическим подходом к описанию угроз безопасности информации угроза как потенциально или реально

существующая опасность нанесения ущерба деятельности ФСВНГ, в том числе за счет нарушения конфиденциальности информации, используемой в интересах реализации этой деятельности, может быть реализована при наличии источника угрозы (нарушителя), уязвимостей как факторов, обусловливающих возможность ее реализации, способа реализации и деструктивного действия в отношении информации как результата реализации угрозы.

Основным фактором, обусловливающим возможность реализации угроз, является использование на объектах радиоэлектронных устройств, которые могут выступать в качестве датчиков ПЭМИ, – источников информации в структуре технического канала ее утечки. При этом способ формирования такого канала, включающего, кроме датчика ПЭМИ, среду их распространения и техническое средство перехвата (приемник), является, по сути, способом реализации угрозы утечки [5, 6].

Однако если возникновение ПЭМИ функционально присуще работе радиоэлектронных устройств объекта информатизации, то утечка информации становится возможной при выполнении ряда условий. Во-первых, эти излучения модулированы информационным сигналом, содержащим сведения, представляющие интерес для нарушителя, то есть на объекте такие сведения обрабатываются. Во-вторых, нарушитель имеет возможность разместить приемник перехвата за пределами контролируемой территории (или в смежном с объектом информатизации помещении в пределах общей контролируемой зоны) на расстоянии, при котором отношение сигнал/шум на его входе превышает уровень чувствительности, или установить в помещении объекта портативное электронное устройство перехвата информации. В-третьих, при этом обеспечивается скрытность применения приемника. Первое условие характеризует динамику реализации процесса обработки информации на объекте информатизации. Его выполнение является событием случайным, так как зависит от случайных временных характеристик (начало, продолжительность, окончание) реализации этого процесса. Второе условие характеризует энергетику технического канала утечки информации, являющегося, по сути, радиоканалом. Его выполнение зависит от характеристик (протяженности) контролируемой легитимными пользователями территории (контролируемой зоны) и характеристик применяемого для перехвата информации приемника – чувствительности и полосы пропускания. Третье условие характеризует динамику действий нарушителя по применению приемника перехвата (или установке закладочного устройства) с учетом обеспечения скрытности как в пределах контролируемой зоны, так и на территории, прилегающей к этой зоне. Его выполнение также является событием случайным, так как, во-первых, зависит от выполнения первого условия, во-вторых, от правильности выбора нарушителем приемника перехвата информации с техническими характеристиками, обеспечиваю-

щими выполнение второго условия и массо-габаритными характеристиками, обеспечивающими скрытность его применения, в том числе с учетом применения мер защиты информации.

Несмотря на то, что в действующих нормативных документах, например, ФСТЭК России, отмечается необходимость обеспечения эффективного противодействия угрозам утечки информации, не содержащей сведений, составляющих государственную тайну, за счет ПЭМИ, в настоящее время требования и меры по ее защите регламентируются лишь в части ограничения энергетики технического канала утечки путем превентивного применения пассивных и активных мер защиты, направленных на уменьшение отношения сигнал/шум на границе контролируемой зоны, то есть на входе приемника перехвата информации ниже уровня его чувствительности.

Методическое обеспечение выбора мер защиты информации и оценки ее защищенности от утечки за счет ПЭМИ сегодня ориентировано только на учет энергетических характеристик ПЭМИ на основе расчетно-измерительных методик расчета требуемых размеров контролируемой зоны вокруг объекта информатизации. При этом оценка защищенности сводится к сравнению рассчитанных значений с реально обеспечиваемыми. На этом основании принимается решение о необходимости и возможности применения мер защиты. Как показывают исследования, проведенные, например, ведущими учеными ГНИИИ ПТЗИ ФСТЭК России эти методики не учитывают условия реализации перехвата информации по ПЭМИ, характеризующие динамику параллельно реализуемых и взаимосвязанных процессов обработки информации на объекте информатизации и ее перехвата нарушителем по техническим каналам, возникающим за счет ПЭМИ. Учет такой динамики может не только существенно повлиять на защищенность информации от утечки, но и изменить требования к защите. Однако для такого учета необходимы новые показатели и математические модели. До настоящего времени показатели и модели, учитывающие указанные условия и факторы, не разрабатывались.

Различные методологические подходы к защите информации от утечки по техническим каналам вообще и по каналам, возникающим за счет ПЭМИ, в частности, отражены в большом числе работ известных специалистов в области информационной безопасности (В. Б. Авдеев, В. Г. Герасименко, С. В. Скрыль, Н. Н. Толстых, А. А. Хорев, А. А. Шелупанов и др.). Однако в их трудах практически отсутствуют исследования по оценке защищенности информации от утечки, связанные с необходимостью представления в формализованном виде разнородных параллельно реализуемых и взаимосвязанных процессов передачи информации между легитимными пользователями на ОИ, перехвата этой информации нарушителем по техническим каналам за счет ПЭМИ и ее защиты от перехвата. В ряде исследований такая оценка осуществлялась на

качественном уровне на основе нечетких суждений с использованием, например, функциональных моделей. При этом вероятностно-временной характер и взаимосвязи исследуемых процессов обусловливали сложность учета динамики их реализации при разработке аналитических моделей для численной оценки защищенности информации от утечки. Отсутствие учета фактора времени, характеризующего указанную динамику, приводит к тому, что такая оценка оказывается завышенной.

Применение для анализа указанных процессов имитационных моделей, а также аппарата Марковских и полумарковских процессов в этом случае ограничено.

В связи с этим наиболее целесообразным для аналитического моделирования исследуемых процессов перехвата информации с учетом времен их реализации является применение аппарата составных сетей Петри–Маркова, ранее применявшегося для количественной оценки эффективности защиты информации от несанкционированного доступа в компьютерных системах и в информационных системах электронного документооборота. Однако возможности применения этого аппарата для моделирования процессов защиты информации на ОИ от утечки по ПЭМИ ранее не рассматривались.

При решении данной задачи необходимо разработать описательные и функциональные модели, а на их основе – адекватные аналитические модели формализованного представления исследуемых процессов с целью корректного использования аппарата сетей Петри–Маркова в интересах оценки защищенности информации от утечки по ПЭМИ [2-4, 9].

При разработке описательных моделей формируется обобщенное описание процессов передачи информации на объектах различного типа, определяются задачи, решаемые в процессе их реализации, содержание и условия реализации и, таким образом, определяются обобщенные исходные данные об объекте, необходимые для формирования функциональных моделей этих процессов, а также процессов перехвата обрабатываемой информации по техническим каналам, возникающим за счет ПЭМИ структурных элементов этих объектов [7].

При этом при описании реализации информационных процессов необходимо учитывать основные факторы, определяющие логические условия и случайный характер времен их реализации, такие как вид информации в ее источнике, вид сигналов (акустические колебания воздушной среды, колебания электрического тока в аналоговом и цифровом виде), используемых в качестве ее материальных носителей, и их энергетические (амплитуда) и частотные характеристики (спектр), а также динамика изменения этих характеристик (продолжительность переговоров). В качестве условий реализации информационного процесса по передаче информации от источника получателю принято обеспечение свойств обрабатываемой информации, характеризующих ее ценность для

получателя. С этой целью выбор структурных элементов объекта, используемых для обработки информации, осуществляется с учетом обеспечения согласования смежных элементов по энергетике и частотному спектру, что обеспечивается путем согласования выходных (сигнальных) характеристик с входными характеристиками (чувствительность, динамический диапазон и полоса пропускания) предыдущего и последующего структурных элементов объекта соответственно. Динамика реализации информационного процесса характеризуется временными характеристиками его реализации. Кроме того, возникновение ПЭМИ структурных элементов объекта возможно непосредственно при подаче электропитания на его оборудование, однако перехват информации за счет этих ПЭМИ становится возможным при условиях, связанных, во-первых, с наличием в составе объекта радиоэлектронных устройств, которые могут выступать в качестве датчиков (источников) ПЭМИ, во-вторых, с реализацией во время перехвата процесса передачи информации, включающего несколько последовательно реализуемых парциальных процессов и имеющих случайные временные характеристики (начало, продолжительность, окончание, паузы между ними).

Применительно к такого рода угрозам утечки информации сегодня имеются лишь их фрагментарные описания, например, описания радиоэлектронных устройств в составе объектов информатизации, которые могут выступать в качестве датчиков информации в структуре технических каналов ее утечки, описания различного рода сред распространения информативных сигналов (проводных или беспроводных) и используемых для их перехвата технических средств разведки. Это определяет в последующем выбор математического аппарата для разработки математических моделей рассматриваемых процессов (аппарата составных сетей Петри-Маркова) [4, 8].

При разработке функциональных моделей рассматриваются различные варианты последовательно и параллельно выполняемых нарушителем действий по перехвату информации за счет ПЭМИ радиоэлектронных устройств на объектах информатизации как в условиях отсутствия мер защиты, так и в условиях их применения.

Разработанные модели служат основой для разработки аналитических моделей расчета общего времени реализации перехвата и оценки защищенности информации как способности системы защиты своевремен- но реагировать на угрозы ее утечки по техническим каналам, возникающим за счет такого рода излучений.

Для моделирования при этом рассматриваются типовые для ФСВНГ объекты информатизации: защищаемые помещения, оборудованные средствами звукоусиления и связи, предназначенные для проведения совещаний, переговоров и других мероприятий.

Действия нарушителя по реализации процесса перехвата информации являются вариативными и случайными во времени. При реализации этого процесса нарушитель выбирает место для реализации перехвата, развертывает

приемник перехвата, настраивает его, инициирует закладочные устройства, если они установлены, и начинает перехват, если реализация информационного процесса на ОИ уже началось, или ждет начала его реализации и далее осуществляет перехват. Одновременно нарушитель осматривает территорию в целях обнаружения ГБР. Если ГБР обнаруживается нарушителем, то он или прекращает перехват и покидает территорию, или игнорирует появление ГБР и лишь при ее приближении прячет технические средства перехвата информации.

Динамика действий на ОИ характеризуется временными характеристиками, во-первых, подготовки и реализации информационного процесса, во-вторых, применения мер защиты.

Соответственно требуется разработать две математические модели оценки защищенности информации от угроз ее утечки в рассматриваемых условиях по показателям сравнения возможностей реализации угроз без применения и в условиях применения мер защиты

В дальнейшем на основе разработанных моделей можно уже осуществить оценку защищенности информации от угроз ее утечки за счет ПЭМИ по показателям, определяющим возможность реализации угроз.

Модель анализа указанных возможностей на основе аппарата сетей Пети-Маркова впервые позволяет учесть фактор времени при обосновании сроков применения мер защиты речевой информации при планировании и проведении мероприятий конфиденциального характера.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ЛИТЕРАТУРЫ

1. Авсентьев О.С. Исследование динамических характеристик процессов формирования технических каналов утечки информации по побочным электромагнитным излучениям радиоэлектронных устройств объектов информатизации и обеспечения защищенности информации от утечки / О. С. Авсентьев, А. О. Авсентьев, А. Г. Кругов. // Вестник Воронежского института МВД России. – 2018. – № 2. – С. 15–29.
2. Авсентьев О. С. Структурно-логическое представление процесса передачи информации на объектах информатизации / О. С. Авсентьев, А. В. Заряев, А. Г. Кругов. // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 22–32.
3. 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.
4. Игнатьев, В. М. Сети Петри–Маркова / В. М. Игнатьев, Е. В. Ларкин. – Тула : ТулГТУ, 1994. –с. 163.
5. Кругов А.Г. Исследование динамики процесса реализации технического канала утечки информации за счет побочных электромагнитных

излучений радиоэлектронных устройств объекта информатизации / А. Г. Кругов. // Информационные системы и технологии ИСТ – 2020 : сборник материалов международной научно-технической конференции. – Нижний Новгород : Нижегородский государственный технический университет им. Р. Е. Алексеева. –2020. – С. 540–547.

6. Кругов А. Г. Проблемы формирования методического обеспечения защиты информации объектов информатизации от утечки за счет побочных электромагнитных излучений / А. Г. Кругов. // Техника и безопасность объектов уголовно-исполнительной системы : сборник материалов международной научно-практической конференции. – Воронеж : Воронежский институт ФСИН России. – 2020. – С. 304–310.

7. Никулин С. С. Функциональное моделирование как инструмент первичной формализации процессов утечки информации по каналам электромагнитных излучений / С. С. Никулин, А. Г. Кругов. // Охрана, безопасность, связь – 2014 : сборник материалов международной научно-практической конференции. – Воронеж : Воронежский институт МВД России. – 2015. – С. 75–78.

8. Язов Ю. К. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри–Маркова / Ю. К. Язов, В. В. Тикунов. // Информация и безопасность : научный журнал. – Воронеж : ГОУ ВПО ВГТУ. – 2018. Том 17, вып.3. – С. 464–467.