ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Авсентьев Олег Сергеевич,
доктор технических наук, профессор;
Волнянкина Татьяна Александровна

ПРОБЛЕМЫ ФОРМИРОВАНИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЬЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ ДИНАМИКИ РЕАЛИЗАЦИИ УГРОЗ ЕЕ БЕЗОПАСНОСТИ

PROBLEMS OF FORMING METHODOLOGICAL PROTECTION OF INFORMATION ON OBJECTS INFORMATIZATION OF THE INTERNAL AFFAIRS IN THE CONDITIONS OF THE DYNAMICS OF THE IMPLEMENTATION OF THREATS HER SAFETY

Рассматриваются проблемы совершенствования методического обеспечения защиты информации, используемой в интересах создания объектов информатизации органов внутренних дел. С этой целью предлагается подход к разработке сценариев динамики параллельно реализуемых процессов обработки этой информации и угроз нарушения ее безопасности нарушителем. Предлагается обеспечение защиты этой информации от угроз ее безопасности на основе информационно-сигнализационных систем, а в интересах количественной оценки защищенности применять аппарат сетей Петри-Маркова.

The problems of improving the methodological support for the protection of information used in the interests of creating objects of informatization of internal affairs bodies are considered. To this end, an approach is proposed to develop scenarios for the dynamics of parallel processes of processing this information and threats of violating its security by an intruder. It is proposed to ensure the protection of this information from threats to its security on the basis of information and signaling systems, and in the interests of a quantitative assessment of security, use the apparatus of Petri-Markov networks.

В соответствии с [1] к объектам информатизации (ОИ) в системе органов внутренних дел (ОВД) России могут быть отнесены служебные кабинеты сотрудников, переговорные кабины, помещения информационно-

вычислительных центров, ситуационные центры и др. Особенности такого рода ОИ заключаются в том, что в их информационных системах (ИС) может обрабатываться информация различного уровня конфиденциальности (содержащая сведения, составляющие государственную тайну (ГТ), информация ограниченного доступа, не содержащая сведений, составляющих ГТ (конфиденциальная информация (КИ)), а также информация общего доступа (ОД)). При этом ИС, а также средства их обеспечения могут располагаться в пределах одной контролируемой территории и даже в одном помещении, а обрабатываемая информация может быть представлена в различной форме (речевой, буквенно-цифровой, графической, видео и др.). С учетом указанных обстоятельств возникает ряд проблем защиты этой информации от угроз ее безопасности на различных этапах существования объекта.

1. В соответствии с [2] защита информации, ограниченного доступа, не содержащей сведений, составляющих государственную тайну, при ее обработке на ОИ ОВД обеспечивается на всех этапах их создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер в составе системы защиты (СЗИ), направленных на блокирование всех угроз безопасности информации (УБИ). Однако, формирование СЗИ осуществляется на этапе ее проектирования и разработки, а применение в интересах обеспечения защиты информации, – на этапах эксплуатации и вывода из эксплуатации. При этом сведения о назначении, цели создания ОИ, решаемых задачах в интересах обеспечиваемой деятельности ОВД по различным направлениям [3], об используемых информационных технологиях, о программном и аппаратном обеспечении ИС и т.п., могут представлять интерес для нарушителя с точки зрения реализации УБИ на различных этапах существования объекта.

2. Существующее методическое обеспечение, например, [2, 4], основано на использовании экспертного подхода к созданию ОИ и его СЗИ, не учитывающего, во-первых, динамику реализации информационных процессов по передаче, приему и обработке информации в различных условиях оперативной обстановки, во-вторых, динамику процессов реализации нарушителем угроз как в отношении информации, содержащейся в ИС ОИ, так и в отношении оборудования и программного обеспечения этих ИС. Вместе с тем, учет указанной динамики может не только существенно повлиять на защищенность информации от УБИ, но и изменить требования по защите.

3. Несмотря на то, что, как отмечено в [2] СЗИ должны быть блокированы все УБИ, в том числе, угрозы утечки по техническим каналам, перечень мер защиты от такого рода угроз ограничен применением средств и систем контроля и управления доступом и организацией контролируемой зоны (КЗ). При этом выполнение требований, указанных в нормативно-методическом документе [5], осуществляется на основе временных расчетно-измерительных методик, также не учитывающих динамику выполняемых нарушителем дей-

ствий по формированию технического канала утечки информации (ТКУИ) [6, 7].

4. Применение экспертных методов не позволяет обеспечить, во-первых, корректность обоснования организационных и технических решений в интересах создания ОИ и его СЗИ, во-вторых, корректность оценки защищенности информации, обрабатываемой на ОИ рассматриваемого типа при проведении аттестационных испытаний на соответствие требованиям о защите информации.

5. Применение других методов оценки, например, на основе функциональных, имитационных моделей или количественной оценки с использованием аппаратов Марковских или полумарковских процессов, ограничено необходимостью исследования параллельно реализуемых и взаимосвязанных разнородных процессов обработки информации на ОИ, угроз безопасности этой информации и ее защиты от такого рода угроз, в условиях динамики и при наличии различных логических условий их реализации [7, 8].

В этих условиях адекватная оценка защищенности информации на ОИ от УБИ становится возможной с использованием аналитических моделей на основе аппарата сетей Петри-Маркова [9]. Однако, для применения данного аппарата необходимо разрабатывать описательные и функциональные модели реализации исследуемых процессов применительно к конкретному ОИ с учетом особенностей их функционирования в интересах обеспечиваемой деятельности структурных подразделений ОВД.

Указанные обстоятельства свидетельствуют об актуальности совершенствования методического обеспечения технической защиты информации, содержащейся в ИС ОИ ОВД, с учетом перечисленных особенностей.

1. Описание алгоритма формирования комплекса мер защиты информации на ОИ ОВД на основе существующего методического обеспечения. Обобщенное представление алгоритма, иллюстрирующего этапы существования ОИ приведено на рис. 1.

В рамках данного алгоритма могут быть выделены ряд этапов.

E_1 – определение назначения и цели создания ОИ и его СЗИ на основе использования достижений науки и техники, ИС, сетей связи, а также современной информационно-телекоммуникационной инфраструктуры, осуществляемое с учетом обеспечения эффективности деятельности ОВД по соответствующим направлениям в условиях постоянного увеличения объемов потоков обрабатываемой информации в интересах этой деятельности [3].

E_2 – определение форм представления и материальных носителей информации, структурных элементов ОИ, их взаимосвязей, используемых информационных технологий, форм представления, ее материальных носителей, как объекта защиты, а также правовых оснований для защиты, учитывающих различие направлений деятельности и ее значимости для личности, общества и государства (ГТ, КИ или ОД).

E_3 – выявление УБИ, включающее определение источников угроз (ИУ) (нарушителей), уязвимостей в структуре ОИ, которые могут быть использованы нарушителем для их реализации, способов эксплуатации выявленных уязвимостей и деструктивных действий, выполняемых в отношении информации и оборудования ИС ОИ.

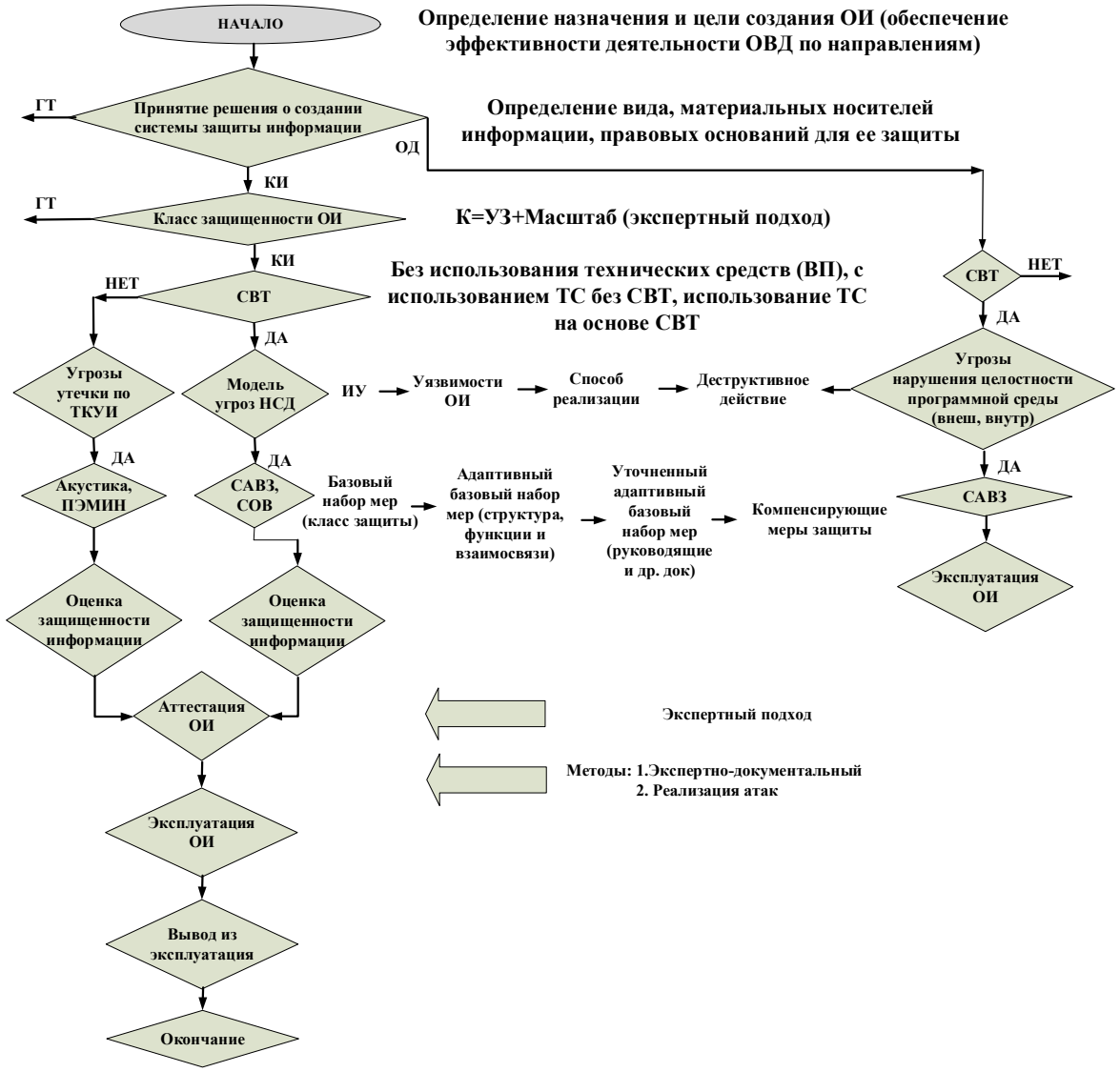

Рис. 1. Обобщенное представление алгоритма существования ИС ОИ и его СЗИ

E_4 – формирование набора мер защиты информации в составе СЗИ, направленных на блокирование всех УБИ, связанных как с реализацией нарушителем угроз несанкционированного доступа (НСД) к информации и оборудованию ИС на основе средств вычислительной техники (СВТ), так и с возможностью ее утечки по техническим каналам (ТКУИ).

E_5 – оценка защищенности информации, как в процессе формирования СЗИ, так и на этапе ее аттестации на соответствие требованиям о защите ин-

формации.

E_6 – эксплуатация ОИ.

E_7 – вывод из эксплуатации.

На каждом из перечисленных этапов необходимые мероприятия и действия выполняются с использованием экспертных методов с привлечением персонала: принимающего решение о создании ИС ОИ и определяющего его категорию (класс защищенности); осуществляющего проектирование и разработку ОИ и его СЗИ с учетом класса защищенности и выявленных УБИ; проводящего аттестационные испытания; эксплуатирующего ИС ОИ и осуществляющего его вывод из эксплуатации.

Так, для выполнения мероприятий на этапе E_1 необходимо иметь сведения, во-первых, об особенностях и условиях деятельности ОВД, в интересах обеспечения, которой создается ОИ, во-вторых, о современных достижениях науки и техники, видах ИС, сетей связи, а также особенностях современной информационно-телекоммуникационной инфраструктуры, используемой на такого рода объектах. Информация, содержащая такие сведения, раскрывающие характер обеспечиваемой деятельности структурных подразделений ОВД, может представлять интерес для нарушителя, заинтересованного в нанесении ущерба, как отдельным гражданам, обществу, так и государству, за счет нарушения основных свойств (конфиденциальности, целостности, доступности) информации, и подлежит защите от угроз ее безопасности.

На этапе E_2 с использованием сведений о формах представления и материальных носителях информации осуществляется выбор структурных элементов ИС ОИ, определяются их взаимосвязи, информационные технологии, элементная база, а также правовые основания для защиты, учитывающие различие направлений деятельности ОВД и ее значимости для личности, общества и государства. Такого рода сведения могут использоваться нарушителем для принятия решения о целесообразности и возможностях реализации УБИ.

Указанные сведения могут также использоваться и на этапе E_3, во-первых, для предварительного выявления уязвимостей ИС ОИ, во-вторых, для определения необходимого технического и программного обеспечения в интересах эксплуатации этих уязвимостей, способов эксплуатации и вида деструктивных действий в отношении информации или оборудования ОИ, как результата реализации УБИ.

На этапе E_4 сведения о сформированном наборе мер защиты информации в составе СЗИ могут быть использованы нарушителем при выполнении попыток преодоления этих мер в процессе реализации УБИ.

2. Описание сценариев реализации информационных процессов в интересах создания ОИ и его СЗИ и процессов реализации угроз в отношении обрабатываемой информации. Информация на этапах $E_1 - E_4$ может обрабатываться в различных формах (речевой, буквенно-цифровой,

графической, видовой и др.), дублироваться в виде руководящих (распорядительных) документов на бумажных или машинных носителях, а ее защита осложняется тем, что система защиты еще не сформирована, контролируемая зона, организация которой является необходимым условием реализации защиты, в ее нормативном определении отсутствует. При этом особенности реализации информационных процессов (ИПр) по передаче, приему, обработке и хранению различной информации заключаются, во-первых, в их фрагментарности, во-вторых, в случайном характере их временных характеристик.

Так формирование некоторого руководящего документа (приказа по подразделению ОВД о создании ОИ, акта классификации ИС в составе объекта и др.) осуществляется в результате многократного обсуждения в речевой форме (например, на совещаниях) соответствующих вопросов экспертами. Иллюстрация соответствующего сценария формирования документа такого рода приведен на рис. 2.

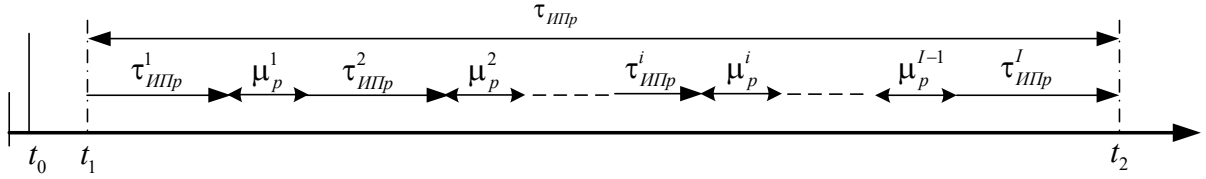

Рис. 2. Иллюстрация сценария формирования распорядительного документа (приказа), регламентирующего необходимость создания ОИ и его СЗИ

На рис. 2 используются следующие обозначения:

t_0 – время начала рабочего дня; t_1 – время начала реализации ИПр (совещания), связанного с подготовкой документа; t_2 – время окончания ИПр (совещания); $\tau^1_{ИПр}$, $\tau^2_{ИПр}$, …, $\tau^I_{ИПр}$ – продолжительности реализации частных процессов (выступлений участников совещания); $\tau_{ИПр}$ – продолжительность всего процесса (до принятия решения) о создании ОИ и его СЗИ; μ^1_P – μ^{I-1}_P – продолжительности пауз между выступлениями участников совещания, включая продолжительность перерыва (перерывов) в процессе мероприятия (совещания).

Приведенные на рис. 2 временные характеристики подпроцессов (и пауз между ними) случайны. Кроме того, процесс ИПр (формирование документа) может продолжаться несколько дней, а по результатам выполнения отдельных подпроцессов ИПр$_i$, i=1, 2, …, I, может быть сформирован рабочий (промежуточный) вариант документа на электронном или бумажном носителе, подлежащий обсуждению. При этом не каждый подпроцесс может содержать сведения, представляющие интерес для нарушителя.

Нарушитель при реализации угроз в отношении информации, обраба-

тываемой в интересах создания ОИ и его СЗИ, вынужден учитывать указанные обстоятельства.

На рис. 3 по аналогии с [6] приведена иллюстрация соответствующего сценария действий нарушителя, реализующего процесс реализации угроз в отношении информации, используемой в интересах создания ОИ и его СЗИ.

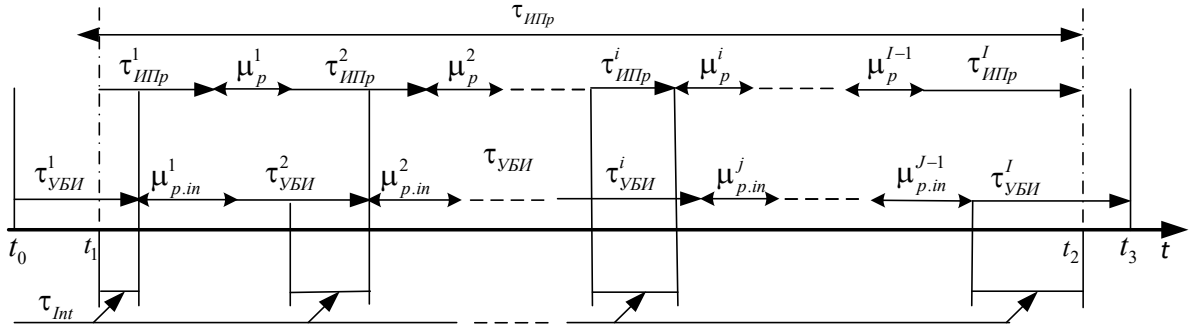

Рис. 3. Иллюстрация сценария действий нарушителя, реализующего угрозы в отношении информации, используемой в интересах создания ОИ и его СЗИ.

На рис. 3 используются следующие обозначения процесса реализации нарушителем УБИ:

$\tau^j_{УБИ}$, $\tau_{УБИ}$ – продолжительности j-го, $j=\overline{1,J}$, временного интервала и общего времени реализации нарушителем угроз в отношении информации, обрабатываемой в интересах создания ОИ и его СЗИ, соответственно;

$\mu^j_{p.in}$ – продолжительность j-го временного интервала между эпизодами реализации нарушителем подпроцессов угроз безопасности в отношении информации, обрабатываемой в интересах создания ОИ и его СЗИ;

τ_{Int} – временные интервалы, соответствующие совпадениям процессов реализации нарушителем УБИ и реализации частных подпроцессов ИПр.

В случае, когда нарушитель включен в состав рабочих групп сотрудников, привлеченных к разработке документов в интересах создания ОИ и его СЗИ, интервалы τ_{Int} могут совпадать с интервалами $\tau^i_{ИПр}$.

Очевидно, что временные характеристики процесса реализации нарушителем УБИ также случайны, а временные интервалы τ_{Int} могут изменяться от 0 до $\tau^i_{ИПр}$.

На рис. 1 и 2 приведены общие описания сценариев реализации взаимосвязанных процессов ИПр и УБИ. Для каждого конкретного объекта подразделения ОВД сценарии будут в существенной степени отличаться. Это обстоятельство обусловливает сложность описания сценариев динамики реализации исследуемых процессов и их взаимосвязей в интересах оценки защищенности информации (в том числе угроз ее утечки по техническим каналам, по аналогии с [6]) и формирования СЗИ.

3. Защита информации на ОИ ОВД на основе информационно-

сигнализационных систем. В условиях, рассмотренных в разделах 1 – 3 данной статьи, адекватная оценка защищенности информации, используемой в интересах создания ОИ и его СЗИ на основе только лишь экспертных методов становится невозможной. Это связано, во-первых, с отсутствием на этапах $E_1 - E_4$ системы защиты информации, обрабатываемой на объектах ОВД, в соответствии с требованиями действующего нормативного методического обеспечения, во-вторых, недостаточной проработкой вопросов оценки защищенности информации, используемой в интересах создания ОИ и его СЗИ, в условиях динамики параллельно реализуемых и взаимосвязанных процессов ее обработки и угроз безопасности. в структуре подразделения ОВД.

Вместе с тем, следует отметить, что здания и сооружения территориальных подразделений ОВД, в которых размещаются ОИ, как правило, оборудованы средствами и системами охранного мониторинга (СОМ), в современном их исполнении относящимися к информационно-сигнализационным системам (ИСС). Указанные системы могут использоваться для защиты информации, содержащей сведения, используемые в интересах создания ОИ и его СЗИ. Однако, исследования, связанные с оценкой защищенности информации в этих условиях, до настоящего времени не проводились.

ИСС используются подразделениями вневедомственной охраны для обеспечения безопасности охраняемых объектов от противоправных и преступных посягательств на материальные и духовные ценности собственников объектов. В их состав включаются: системы и средства инженерно-технической укрепленности (ИТУ); системы контроля и управления доступом (СКУД); системы охранно-пожарной сигнализации; системы видеонаблюдения; СВТ и другие технические средства получения и передачи информации в интересах управления ИСС. В качестве объекта защиты рассматриваются, в первую очередь, материальные ценности. Это обусловливает особенности описания угроз их безопасности. Различные сценарии реализации такого рода угроз связаны с возможностями злоумышленников, как источников угроз, по преодолению рубежей охраны и получению доступа в помещения, в которых хранятся материальные ценности, с целью их хищения за время меньшее, чем время блокирования угрозы силами быстрого реагирования (СБР) в составе системы безопасности.

Поскольку деятельность ОВД по своей сути является информационной, то в качестве объекта защиты ИСС в зданиях и сооружениях системы ОВД, в первую очередь, рассматриваются информационные ресурсы, используемые сотрудниками подразделений ОВД в различных условиях оперативной обстановки. Применение ИСС на объектах ОВД, в первую очередь, направлено на противодействие проникновению на территорию подразделения ОВД нарушителей, имеющих противоправные цели по реализации УБИ (в том числе информации, используемой в интересах создания ОИ), циркулирующей на этих объектах, путем реализации мер контроля и

управления доступом в здания и помещения территориального подразделения ОВД.

До настоящего времени вопросы защиты информации, используемой в интересах создания ОИ и его СЗИ, с использованием средств ИСС не рассматривались. При этом адекватная оценка защищенности этой информации от УБИ становится возможной с использованием аналитических моделей на основе аппарата сетей Петри-Маркова [9]. Однако, для применения данного аппарата необходимо разрабатывать описательные и функциональные модели реализации исследуемых процессов применительно к конкретному ОИ с учетом особенностей их функционирования в интересах обеспечиваемой деятельности структурных подразделений ОВД.

Представленные описания сценариев параллельно реализуемых и взаимосвязанных процессов обработки информации, используемой в интересах создания ОИ и его СЗИ, 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, привлеченных к 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 [9]. Разработка таких моделей является предметом дальнейших исследований авторов.

ЛИТЕРАТУРА

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

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

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

4. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

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

6. Авсентьев А. О., Вальде А. Г. Вербальная модель угроз утечки информации по техническим каналам в процессе создания объектов информатизации // Вестник Воронежского института МВД России. 2022. № 2. С. 65-75.

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

8. Авсентьев О. С. 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

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