УДК 004.056:519.1

О.С. Авсентьев, Э.А. Томилова

Модели адаптивного управления защитой информации в процессе создания государственной информационной системы

Рассмотрены проблемные вопросы разработки моделей адаптивного управления защитой информации в государственной информационной системе в процессе создания системы ее защиты, позволяющих учитывать изменения форм представления защищаемой информации, совокупность условий динамики ее обработки и факторов, создающих опасность реализации угроз утечки по техническим каналам. Разработаны описательные модели исследуемых процессов. Обоснована возможность учета указанных изменений и условий на основе системы адаптивного управления защитой информации, создаваемой по централизованному принципу и обеспечивающей управление в двух уровнях путем усиления мер защиты в соответствии с изменениями состава объекта защиты, внутренних и внешних факторов, характеризующих динамику функционирования такой системы, а также направлений решения проблемных вопросов оценки ее эффективности. Для расчета показателей оценки эффективности управления защитой информации на этапах создания информационной системы в защищенном исполнении, учитывающих фактор времени и различные логические условия управления защитой, предложено применение аппарата составных сетей Петри–Маркова. Разработаны блок-схемы циклов управления для двух уровней, которые рассматриваются в качестве основы для формирования графов составных сетей Петри–Маркова.

Ключевые слова: информационная система в защищенном исполнении, система адаптивного управления защитой информации, угроза утечки информации, условия и факторы, эффективность управления защитой информации.

DOI: 10.21293/1818-0442-2024-27-4-61-73

Защита информации (ЗИ), не содержащей сведений, составляющих государственную тайну, является составной частью работ по созданию и эксплуатации информационной системы в защищенном исполнении (ИСЗИ), создаваемой для обеспечения деятельности какой-либо организации государственного сектора (далее – организации), и должна обеспечиваться на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия мер защиты, направленных на блокирование угроз безопасности информации (УБИ) [1]. При этом если на этапах эксплуатации и вывода из эксплуатации защита осуществляется на основе сформированной и аттестованной системы ЗИ (СЗИ) в помещениях, оборудованных в соответствии с требованиями к защищаемым помещениям (ЗП), то на предшествующих этапах такая СЗИ еще не сформирована и возникает ряд проблемных вопросов, связанных с выбором мер защиты в условиях изменений состава объекта защиты и динамики реализации УБИ, обрабатываемой при выполнении работ на каждом из этих этапов. Однако в [1, 2] в явном виде разделение процесса создания ИСЗИ на этапы не приведено, перечислены лишь мероприятия, проводимые в интересах ее создания.

В [3] такое разделение приведено, однако при выполнении работ в рамках каждого из этапов не предусмотрены меры по защите информации. В связи с указанными обстоятельствами на этапах, предшествующих эксплуатации ИСЗИ, не представляется возможным корректное определение информации, обрабатываемой при выполнении работ на различных этапах, как объекта защиты. Кроме того, часть такого рода работ выполняется сотрудниками (работниками) организации, как представителями заказчика [2, 3], во-первых, часто не имеющими соответствующей квалификации, во-вторых, обрабатывающими информацию на каждом из этапов в помещениях, как правило, не оборудованных в соответствии с требованиями к ЗП. Это обусловливает трудности по разработке модели УБИ, учитывающей изменения видов обрабатываемой информации, материальных носителей, состава используемого оборудования и динамику реализации информационных процессов по ее обработке.

Следует отметить, что в качестве негативного последствия реализации УБИ в процессе создания ИСЗИ рассматривается утечка информации, обрабатываемой на каждом из этапов [4]. При этом получение доступа к содержанию перехваченной информации может использоваться нарушителем для реализации УБИ, обрабатываемой на этапе эксплуатации ИСЗИ, например, путем преодоления мер защиты в составе созданной СЗИ, и, как следствие, для нанесения ущерба деятельности организации. Поскольку перехват информации нарушителем может осуществляться путем формирования каналов утечки, в том числе технических (ТКУИ), то в состав объекта защиты следует включать и помещения, в которых осуществляется обработка защищаемой информации, а объект защиты целесообразно рассматривать как объект информатизации (ОИ).

В связи с тем, что обработка информации, используемой при выполнении работ на каждом этапе создания ИСЗИ в составе ОИ, осуществляется во времени, соответствующие информационные процессы характеризуются случайными временными характеристиками. Это обусловливает трудности оценки защищенности информации и эффективности приме-

няемых мер защиты [5] на каждом из этапов. Результаты обработки информации на текущем этапе используются в качестве исходных данных на последующем этапе. При этом изменяются содержание обрабатываемой на ОИ информации, оборудование, используемое для ее обработки, как объекты защиты, и перечень УБИ, что обусловливает необходимость применения дополнительных, соответствующих данным изменениям мер защиты.

В настоящее время для выбора и применения мер защиты в процессе создания ИСЗИ на ОИ проводится комплекс мероприятий [1], реализуемых предварительно группой сотрудников структурного подразделения или назначенным должностным лицом организации, ответственными за защиту информации. При этом управление этой группой осуществляется по централизованному принципу, например, руководителем организации или сотрудником, ответственным за организацию и проведение мероприятий в интересах создания ИСЗИ в составе ОИ.

В рассмотренных выше условиях организацию и проведение этих мероприятий некорректно считать управлением защитой информации, обрабатываемой на этапах создания такого рода ИС, поскольку не определены объекты и цели защиты, условия и факторы, создающие потенциально или реально существующую опасность реализации нарушителем угроз утечки защищаемой информации, цели защиты, критерии оценки защищенности информации и эффективности применяемых мер защиты.

Существующее методическое обеспечение, например [1–3], не позволяет, во-первых, учесть указанные изменения объекта защиты, условия, характеризующие динамику параллельно реализуемых процессов обработки информации, используемой в интересах создания ИСЗИ, и угроз ее утечки, во-вторых, применить адекватные меры защиты по блокированию этих угроз. Выходом из создавшейся ситуации представляется разработка в составе создаваемой СЗИ системы (подсистемы) адаптивного управления защитой информации (САУЗИ), обеспечивающей управление применением различных организационных и технических мер защиты, направленных на своевременное блокирование угроз утечки информации, обрабатываемой при выполнении работ на различных этапах создания ее СЗИ с учетом рассмотренных изменений и условий.

В этом случае система решений в ходе управления защитой распределяется по направлениям, связанным с обработкой информации различного вида и ее защитой от утечки на каждом этапе. В интересах поддержки принятия этих решений целесообразно создание специализированного программно-аппаратного комплекса, используемого для управления множеством датчиков и аппаратных или программно-аппаратных средств защиты, функционирующих в условиях динамики изменения обстановки и распределенных по территории ОИ. Эффективность защиты, как степень соответствия результата защиты поставленной цели, в этих условиях следует рассматривать с учетом того, насколько эффективно управление САУЗИ в достижении цели защиты.

В настоящее время исследования, связанные с построением систем управления, используемых в различных сферах деятельности, в основном посвящены развитию теории управления, математических методов описания процессов управления, архитектуры построения управленческих циклов в целом, методов и средств коммуникации их структурных элементов, поддержки взаимосвязей между ними и др. [6–8]. Однако вопросы применения САУЗИ для управления защитой информации, обрабатываемой при выполнении работ на этапах создания ИСЗИ в составе ОИ, от утечки по техническим каналам и реализации предложенного принципа адаптивного управления защитой на ее основе в связи с необходимостью решения ряда проблемных вопросов оценки эффективности САУЗИ и эффективности управления ею до настоящего времени даже не рассматривались.

Данная статья посвящена исследованию возможности применения существующего аппарата теории управления в интересах обоснования методов управления САУЗИ от утечки по техническим каналам на ОИ в условиях изменения состава объекта защиты, внутренних и внешних факторов, характеризующих динамику функционирования такой САУЗИ, а также обоснования направлений решения проблемных вопросов оценки эффективности такого рода системы и эффективности управления ею.

Описание информационных процессов по обработке информации на различных этапах создания ИСЗИ как объектов защиты

На этапах, предшествующих эксплуатации ИСЗИ, проводятся следующие мероприятия:

– e_1 – формирование требований к защите информации, содержащейся в информационной системе;

– e_2 – разработка системы защиты информации;

– e_3 – внедрение системы защиты информации;

– e_4 – аттестация информационной системы по требованиям защиты информации и ввод ее в действие.

Часть работ на этапах $e_1 \div e_4$ по формированию требований к ИСЗИ, ее разработке, организации внедрения, аттестации на соответствие требованиям безопасности информации и вводу в действие в соответствии с [1, 4] осуществляется обладателем информации (заказчиком) в условиях отсутствия сформированной СЗИ, соответствующей требованиям о защите информации.

Нарушение конфиденциальности информации, обрабатываемой сотрудниками организации при выполнении работ на этапе e_1 и содержащей различные сведения ограниченного доступа [1, 4], может быть использовано нарушителем как при разработке сценариев реализации угроз ее утечки по техническим каналам на этапах $e_2 \div e_4$, так и при реализации УБИ, обрабатываемой на этапе эксплуатации ИС.

Сценарии реализации угроз могут быть скорректированы нарушителем для соответствующих способов их реализации применительно к конкретным объектам воздействия, последовательности выполняемых действий, привлечению необходимых сил и

средств, соответствующих его возможностям (потенциалу), а также планированию выделяемых ресурсов для реализации угроз как в отношении этой информации, так и оборудования создаваемой ИСЗИ.

На этапе e_2 сотрудниками подразделения обрабатываются сведения: о составе пользователей, процессов и других субъектов доступа, объектов, подлежащих защите в ИСЗИ в составе ОИ; о правилах разграничения, методах контроля и управления доступом; об уязвимостях ИС, которые могут привести к возникновению УБИ; о мерах ЗИ, включаемых разработчиком в состав СЗИ, о ее структуре и размещении элементов в составе ОИ. Нарушение конфиденциальности сведений о формируемой СЗИ может быть использовано нарушителем для обхода мер защиты при реализации УБИ на этапе эксплуатации ИСЗИ и ОИ [4].

Раскрытие сведений, обрабатываемых сотрудниками подразделения при внедрении ИСЗИ на этапе e_3 и содержащихся в разработанных организационно-распорядительных документах по ЗИ, о результатах предварительных испытаний и опытной эксплуатации СЗИ, об уязвимостях ИСЗИ, об уточнении модели УБИ и принятии (дополнении) мер по их блокированию, позволит нарушителю на этапе эксплуатации ИСЗИ скорректировать сценарии реализации УБИ с учетом обхода дополненных, в том числе организационных, мер защиты в составе скорректированной СЗИ.

На этапе e_4 при проведении аттестационных испытаний ИСЗИ осуществляется анализ информации, содержащейся в документах, разработанных на этапах $e_1 \div e_3$, в части их соответствия нормативным требованиям [1]. Раскрытие сведений, содержащихся в указанных документах, может быть использовано нарушителем с целью нарушения функционирования оборудования ИСЗИ, а также реализации УБИ на этапах ее эксплуатации и вывода из эксплуатации.

Как показано в [4], в интересах создания ИСЗИ в составе ОИ обрабатывается информация как в форме документов на бумажных или электронных носителях, так и в речевом виде. В первом случае при реализации процессов разработки этих документов могут использоваться средства вычислительной техники (СВТ), имеющиеся в распоряжении сотрудников организации, а также соответствующие документы на бумажных носителях. Обсуждение и утверждение руководителем разработанных документов осуществляются на совещаниях в речевой форме. В [4] обосновано представление такого рода процессов в виде потоков событий, содержащих сообщения сотрудников организации, выполняющих работы в интересах создания ИСЗИ.

На рис. 1 в качестве примера приведена временная диаграмма реализации процессов по обработке информации в речевой форме при обсуждении результатов выполнения работ на этапах $e_1 \div e_4$ [4].

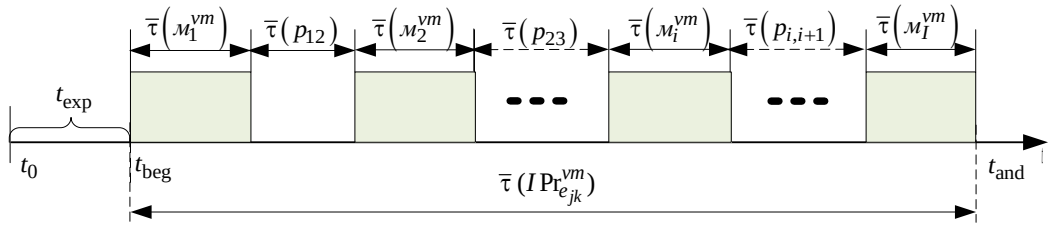

Рис. 1. Временные диаграммы реализации процессов по обработке информации в речевой форме при обсуждении результатов выполнения работ на этапе e_1 «Формирование требований к ЗИ»

На рис. 1 используются следующие обозначения: t_0 – время начала рабочего дня в организации; t_{exp} – время ожидания начала совещания (мероприятия); t_{beg} и t_{and} – времена начала и окончания совещания, соответственно; $\overline{\tau}\left(м_i^{vm}\right), i=\overline{1,I}$, – средняя продолжительность речевого сообщения массива $м_i^{vm}$ i-го, участника совещания; $\overline{\tau}\left(p_{i,i+1}\right), i=\overline{1,I-1}$ – средняя продолжительность паузы между выступлениями i-го и $(i+1)$-го участников совещания; $\overline{\tau}\left(I\,\text{Пр}_{e_{jk}}^{vm}\right)$ – среднее время реализации информационного процесса $I\,\text{Пр}_{e_{jk}}^{vm}$ $\left(e_{jk}\right)$ по обсуждению результатов выполнения k-й работы j-го этапа создания ИСЗИ, $k=\overline{1,K}$, $j=\overline{1,J}$.

Временные диаграммы, аналогичные представленной на рис. 1, могут быть использованы для иллюстрации процессов обработки информации в интересах выполнения работ на различных этапах создания ИСЗИ.

Нарушение конфиденциальности информации, обрабатываемой на этапах создания ИСЗИ, в случае ее перехвата, является результатом реализации нарушителем угроз ее утечки, во-первых, по каналам утечки с использованием технических средств или без их использования, во-вторых, за счет получения физического или логического (через ЛВС или интернет) доступа к компьютерам, используемым для создания необходимых документов [4]. Как показано в [5] угроза утечки информации может быть реализована при выполнении ряда логических условий: наличие сформированного нарушителем канала утечки; соответствие условий его формирования требованиям скрытности применения средств (в том

числе технических) перехвата защищаемой информации, обеспечивающих возможность приема побочных информативных сигналов структурных элементов ИС и отображения содержащейся в параметрах этих сигналов информации, представляющей интерес для нарушителя; обработка этой информации на ОИ в течение времени реализации ее перехвата. Указанные обстоятельства обусловливают динамику реализации такого рода угроз [5].

Для применения адекватных мер защиты необходимо проводить оценку угроз утечки защищаемой информации на каждом из этапов создания ИСЗИ [9]. Более того, в соответствии с [9] такая оценка должна проводиться «систематически». При этом возникают проблемные вопросы, связанные с неопределенностью показателей и критериев оценки, а также самого понятия систематичности. Кроме того, возникают существенные трудности оценки, связанные, во-первых, со спецификой описания изменений защищаемой информации как объекта защиты от угроз ее утечки, во-вторых, с описанием условий и факторов, создающих потенциальную или реально существующую опасность реализации нарушителем этих угроз. Указанные обстоятельства обусловливают необходимость решения указанных вопросов при разработке моделей управления САУЗИ ИСЗИ, оценке эффективности такого рода системы и эффективности управления ею.

Описание динамики процессов реализации угроз утечки информации, обрабатываемой на этапах создания ИСЗИ

В соответствии с современным подходом к оценке защищенности информации и эффективности ее защиты на всех этапах существования ИСЗИ необходимо проводить оценку (анализ) УБИ, включающую следующие мероприятия [10].

1. Определение состава защищаемой информации и характеристик ОИ, в пределах которого осуществляется ее обработка. Обработка речевой информации массивов $м_i^{vm}$ (см. рис. 1) может осуществляться как без использования технических средств, так и с использованием средств усиления и воспроизведения звука (при проведении совещаний на больших ОИ) [5]. Разработка документов в интересах создания ИСЗИ осуществляется с использованием компьютеров, как автономных, так и включенных в локальную вычислительную сеть (или сеть Internet).

2. Определение возможных источников угроз. Источником угрозы утечки информации могут быть как внутренние, так и внешние нарушители, а также внешние нарушители, выступающие в сговоре с внутренними [4, 9]. При этом способом реализации угрозы является формирование нарушителем канала утечки информации.

3. Выявление уязвимостей, которые могут эксплуатироваться нарушителем при реализации угроз утечки информации. В качестве основных рассматриваются уязвимости, связанные с использованием для обработки защищаемой информации оборудования, элементы которого могут выступать в качестве датчиков информации в составе ТКУИ.

4. Определение состава возможных угроз утечки информации о создаваемой ИСЗИ. При этом необходимо учитывать то обстоятельство, что угрозы считаются разными при их отличии даже в одном из элементов описания: источник угрозы, эксплуатируемая уязвимость, объект воздействия, сценарий реализации.

5. Определение возможностей реализации такого рода угроз и оценка ущерба от их реализации. Информация, представляющая интерес для нарушителя, может содержаться в одном или нескольких перехваченных речевых сообщениях или создаваемых документах, состав которых при оценке угроз, как правило, неизвестен.

6. Определение перечня актуальных УБИ (модели УБИ) на каждом из этапов создания ИСЗИ.

Одним из существенных факторов, влияющих на результаты оценки угроз утечки информации, обрабатываемой на различных этапах создания ИСЗИ, защищенности этой информации от утечки и эффективности применяемых мер защиты является фактор времени, характеризующий динамику реализации такого рода угроз и применяемых мер в условиях динамики реализации информационных процессов, например, $I\,\mathrm{Pr}_{e_{jk}}^{vm}$ (см. рис. 1), изменения структурных элементов создаваемой ИС, используемых для обработки информации, представленной в различном виде на различных этапах создания ИСЗИ.

В результате проведения перечисленных мероприятий по оценке угроз утечки информации формируется модель угроз. В настоящее время формирование модели угроз утечки информации, не содержащей сведений, составляющих государственную тайну, осуществляется в соответствии с требованиями, приведенными, например, в [11], а оценка защищенности информации от утечки осуществляется путем измерений уровней информативных сигналов в опорных точках вокруг структурных элементов создаваемой ИС в составе ОИ с использованием расчетно-измерительных методик с последующими расчетами уровней этих сигналов на границе контролируемой зоны (КЗ) ОИ. При этом защищенность информации как способность системы защиты противостоять ее утечке определяется в зависимости от выполнения условий [12]:

$$A_{\mathrm{IS}}/P_N < \mu_{\mathrm{res}}, \quad (1)$$

$$\Delta\tau_{\mathrm{IS}} < \left(\tau_{\mathrm{exp}} + \tau_{\mathrm{и}}\right), \quad (2)$$

$$\Delta f_{IS} > \Delta F_{\mathrm{res}}, \quad (3)$$

где A_{IS}/P_N – отношение (информативный сигнал) / шум на границе КЗ ОИ; μ_{res} – чувствительность технического средства, применяемого нарушителем для перехвата информации; $\Delta\tau_{\mathrm{IS}}$ – продолжительность передачи информации; $\tau_{\mathrm{exp}}, \tau_{\mathrm{и}}$ – времена формирова-

ния нарушителем ТКУИ и реализации перехвата информации соответственно; $\Delta f_{\text{IS}}, \Delta F_{\text{res}}$ – ширина спектра информативного сигнала и полосы пропускания приемника технического средства перехвата (ТСП) информации соответственно.

Защищенность информации определяется как соответствие состава принятых мер защиты информации составу мер, установленному нормативным документом, т.е. от выполнения условий (1)–(3) на границе КЗ ОИ. А применяемые меры защиты либо эффективны в случае выполнения этих условий, либо не эффективны в противном случае [12].

Однако в процессе обработки информации на этапах создания ИСЗИ необходимо учитывать факторы, которые могут повлиять на результаты оценки угроз утечки этой информации, в том числе ее утечки по техническим каналам при реализации перечисленных выше мероприятий:

1. Особенности состава защищаемой информации на каждом из этапов создания ИСЗИ, характеристик ОИ (в том числе размеров КЗ) и динамики реализации процессов обработки этой информации с использованием оборудования различного состава (либо без его использования).

2. Неопределенность сведений о возможностях нарушителя (внутреннего или внешнего) по реализации какого-либо из сценариев перехвата как речевой, так и документальной информации, обусловленных реализацией принципа негласности ведения перехвата информации [5].

3. Неопределенность, случайная направленность и содержание действий нарушителя, выполняемых при реализации различных сценариев перехвата этой информации.

4. Многообразие возможных угроз утечки информации, обрабатываемой на различных этапах создания ИСЗИ, и сложности их оценки в рассматриваемых условиях.

5. Отсутствие в настоящее время методов оценки ущерба при анализе угроз утечки информации, что обусловливает применение принципа неприемлемости любого ущерба [10].

6. Состав актуальных угроз в отношении информации, обрабатываемой на различных этапах создания ИСЗИ, изменяется с учетом того, что угроза считается актуальной, если она может быть реализована и при ее реализации может быть нанесен ущерб обладателю информации [9, 10].

Кроме того, применение расчетно-измерительных методик не позволяет учесть динамику проявления перечисленных факторов при обработке информации в процессе выполнения различных работ даже в рамках отдельного этапа, а также то, что оценку защищенности информации от утечки и эффективность применяемых мер защиты следует проводить с учетом параллельной реализации процессов обработки информации, реализации угроз ее утечки по техническим каналам и применения мер защиты от утечки. При этом отсутствие учета фактора времени приводит, как правило, к завышенным оценкам защищенности информации, поскольку невыполнение условия (1) не означает то, что нарушитель сможет успеть перехватить информативный сигнал в соответствии с (2), а полоса пропускания приемника, используемого в составе ТСП, достаточна для отображения сведений, содержащихся в параметрах этого сигнала.

В соответствии с [4, 9] сценарий определяется как последовательность возможных действий, выполняемых нарушителем, имеющим необходимые ТСП для формирования ТКУИ, или уровень доступа к документам на бумажных носителях или к компьютерам, включенным в ЛВС организации и используемым для создания этих документов и их демонстрации при проведении совещаний. На рис. 2, *б* приведена временная диаграмма, иллюстрирующая один из множества возможных сценариев реализации угрозы утечки речевой информации, соответствующий ситуации, при которой нарушитель имеет возможность периодически применять ТСП в зоне возможного перехвата информации, обрабатываемой в интересах создания ИСЗИ. Динамика реализации процессов ее обработки (рис. 2, *а*) соответствует временной диаграмме, приведенной на рис. 1. Пунктирными линиями выделены фрагменты сообщений в составе информационного процесса $I\,\text{Pr}_{e_{jk}}^{vm}$, которые могут быть перехвачены нарушителем.

На рис. 2, *а* используются такие же обозначения, как и на рис. 1.

На рис. 2, *б* используются следующие обозначения: $\bar{\tau}(CU)$ – среднее время формирования нарушителем канала утечки информации, включающее средние времена выполнения последовательности действий (прибытие в зону возможного приема информативного сигнала, его обнаружение, выбор места, обеспечивающего скрытность применения приемника в составе ТСП, прием сигнала, настройка характеристик приемника, отображение перехваченной информации и др. [5]) в интересах реализации угрозы ее утечки; $\bar{\tau}\left(u_l^{vm}\right), l=\overline{1,L}$ – время реализации l-й попытки перехвата речевого сообщения во время проведения совещания; $\bar{\tau}\left(p_{l,l+1}^{vm}\right)$ – продолжительность паузы между l-й и $(l+1)$-х попытками перехвата речевого сообщения во время проведения совещания; $\bar{\tau}\left(\text{Pr}_u^{vm}\left(e_{jk}\right)\right)$ – средняя продолжительность реализации угрозы утечки речевой информации во время проведения совещания по результатам выполнения работ в процессе e_{jk} этапа e_j формирования ИСЗИ в составе ОИ.

В [5] обосновано, что применение существующих подходов к оценке угроз утечки информации, обрабатываемой на этапах создания ИСЗИ, защищенности этой информации от утечки, эффективности применяемых мер защиты не позволяет обеспечить адекватность указанных оценок.

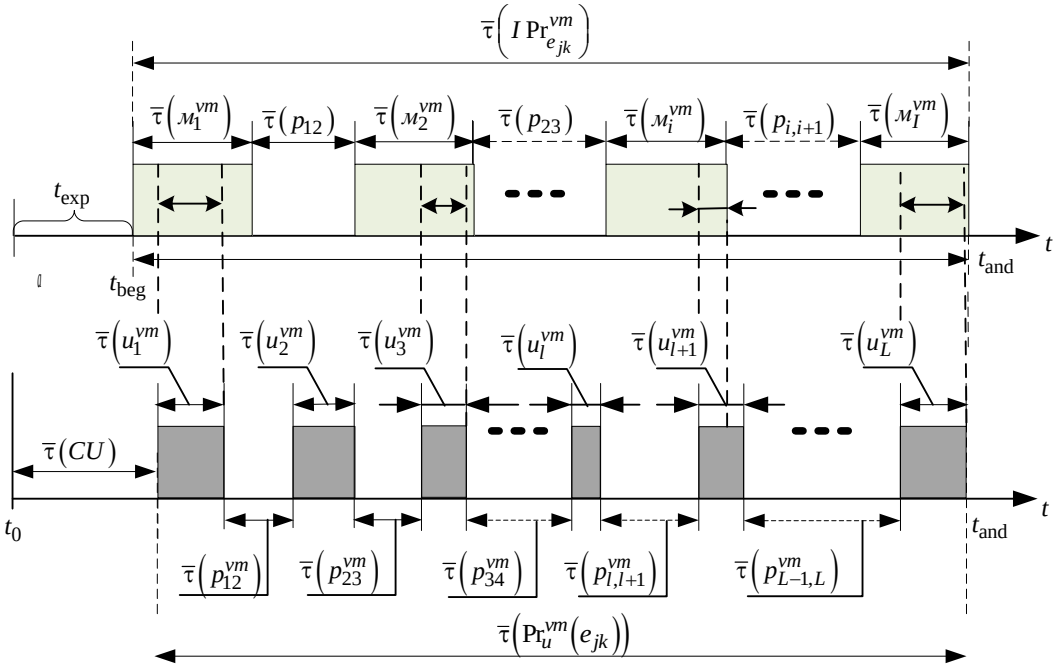

Рис. 2. Временные диаграммы сценария реализации угрозы утечки речевой информации, обрабатываемой при выполнении работ в процессе e_{jk} на этапе e_j, внутренним нарушителем. Без мер защиты

Принципы управления САУЗИ в условиях динамики реализации процессов обработки информации на этапах создания ИСЗИ в составе ОИ, угроз ее утечки по техническим каналам и защиты от утечки

Систему называют адаптивной, если она способна реагировать на изменения внутренних и внешних условий функционирования объекта управления. Управление САУЗИ – это управление применением мер защиты информации в процессе создания ИСЗИ в условиях наличия неполной априорной информации об управляемом процессе (объекте управления), которые изменяются по мере накопления информации и учитываются с целью улучшения качества функционирования системы [6]. САУЗИ подстраивается под условия обработки информации различной физической природы на различных этапах создания ИСЗИ с учетом обстоятельств ее обработки и адекватным образом меняет свое поведение или характеристики, чтобы обеспечить решение стоящих перед нею задач.

В процессе управления САУЗИ могут быть выделены пять этапов, составляющих управленческий цикл: 1) определение цели создания САУЗИ от утечки по техническим каналам и необходимости решения задач управления в различных условиях обстановки; 2) сбор и обработка информации о состоянии объекта защиты в интересах оценки ситуации в условиях динамики управления САУЗИ; 3) принятие решения на выполнение наиболее целесообразных действий в интересах управления процессом функционирования САУЗИ; 4) исполнение принятого решения; 5) контроль исполнения решения [13].

Под управлением САУЗИ от утечки по техническим каналам на ОИ будем понимать организацию процесса формирования органом управления защитой совокупности управляющих воздействий на оборудование объекта и средства защиты, а также команд подразделениям и / или должностным лицам на применение организационных, организационно-технических и технических мер в интересах повышения эффективности защиты информации от утечки на каждом этапе создания ИСЗИ в целом.

С учетом целей выполнения работ, их последовательности и содержания на различных этапах создания ИСЗИ, приведенных в [4], САУЗИ должна обеспечивать решение задач поддержки принятия решений по применению организационных и технических мер защиты информации различной физической природы, обрабатываемой при выполнении работ на каждом из этапов и в процессе создания ИСЗИ в целом, с целью своевременного блокирования угроз ее утечки по техническим каналам.

В соответствии с описанием такого рода угроз меры защиты должны быть направлены, во-первых, на блокирование источника угрозы, выполняющего действия по формированию канала утечки, как на территории ОИ (внутреннего нарушителя), так и на территории, прилегающей к объекту (внешнего нарушителя), во-вторых, на локализацию или скрытие информативных сигналов структурных элементов оборудования, используемого для обработки защищаемой информации, путем применения средств защиты пассивного и / или активного характера соответственно, в-третьих, на противодействие выполнению нарушителями действий по формированию канала утечки в условиях динамики и скрытности выполнения этих действий за счет своевременного их выявления, например, с использованием систем видеонаблюдения, и удаления из зоны возможного перехвата информации силами групп быстрого реагирования (ГБР) [5].

Под организационными понимаются меры по защите информации, предусматривающие установление временных, территориальных и пространственных ограничений на условия использования и режимы работы объекта защиты [14], например, меры, направленные, на поиск и задержание нарушителей на территории ОИ, введение ограничений на посещение помещений объекта и т.п. К организационно-техническим относятся меры организационного характера, реализуемые с применением технических средств, например, контроль и управление доступом на территорию ОИ, обеспечение КЗ, а также поиск закладочных устройств с использованием специальных технических средств и др. К техническим относятся меры с применением технических, программных и программно-технических средств защиты информации пассивного и активного характера [14].

На этапах создания ИСЗИ при отсутствии СЗИ, аттестованной по требованиям о защите информации, в качестве основы для ее формирования могут использоваться меры обеспечения безопасности объектов в составе системы охранного мониторинга (СОМ), включающей совокупность разнородных функционально объединенных датчиков информации (видео-, аудио-, радио-, оптических и др.) о состоянии охраняемого объекта, вычислительных и вспомогательных технических средств ее получения, передачи и хранения в интересах решения задач охраны и предупреждения о возникновении нежелательных ситуаций, создаваемой, как правило, с использованием программно-аппаратных комплексов (ПАК) [15]. Применительно к решению защиты информации, обрабатываемой в интересах создания ИСЗИ как объекта защиты (охраны), меры, реализуемые в составе СОМ, следует рассматривать как превентивно установленные. В процессе решения задач управления в условиях изменения состава объекта защиты на основе анализа собранной и обработанной информации об этих изменениях, о возникновении новых факторов, обусловливающих возможность реализации нарушителем угроз утечки обрабатываемой информации, может быть принято решение на выполнение наиболее целесообразных действий с применением иных дополнительных мер защиты, как организационно-технических, так и технических, в интересах управления процессом функционирования САУЗИ, адаптированных к этим изменениям.

В этих условиях управление САУЗИ осуществляется на двух уровнях (рис. 3).

На первом уровне выбор организационных и организационно-технических мер защиты и управление ими осуществляется только централизованно руководством организации или руководителем подразделения, созданного для проведения работ по созданию ИСЗИ. В качестве объекта управления выступают предварительно установленные меры защиты в составе СОМ, включающей ПАК систем (подсистем) контроля и управления доступом (СКУД), видеонаблюдения, охранной и пожарной сигнализации (СОПС), средства инженерно-технической укрепленности (ИТУ), силы и средства ГБР и др. [14]. С использованием указанных подсистем в составе СОМ, во-первых, обеспечивается КЗ вокруг ОИ, а также контроль и управление доступом на территорию данной зоны. Однако размеры этой зоны могут быть ограничены за счет использования различного рода ограждающих конструкций, усиленных средствами ИТУ: заборов вокруг территории, прилегающей к зданию, принадлежащему организации (с калитками и воротами), контролируемых по периметру с использованием средств СКУД и видеонаблюдения (рубеж охраны *3*); стен, входных дверей, оконных проемов самого здания (рубеж охраны *2*) и помещений, в которых выполняются работы и обрабатывается информация в интересах создания ИСЗИ (рубеж охраны 1) [15].

Для контроля ограждающих конструкций помещений применяются средства СОПС и СКУД. При этом в качестве основных факторов, влияющих на обеспечение защиты информации от утечки, следует рассматривать, во-первых, расположение помещений в пределах здания, во-вторых, архитектурные особенности этого здания (количество этажей, наличие или отсутствие внутреннего двора и др.), в-третьих, размеры территории, прилегающей к зданию и ограниченной заборами, при их наличии или отсутствии, например, в условиях городской застройки.

Указанные факторы, обусловливают выполнение или невыполнение условия (*1*) на границе КЗ, которая может быть реально обеспечена для ОИ. Кроме того, в условиях невозможности обеспечения третьего рубежа охраны важное значение имеют характерные особенности территории, прилегающей ко второму рубежу, в части оценки возможности скрытного применения нарушителем ТСП и выполнения условий (*2*) и (*3*) перехвата информации. В зависимости от вида информации, обрабатываемой при выполнении различных работ в интересах создания ИСЗИ, перечень условий и факторов, создающих опасность реализации угрозы ее утечки, изменяется. В современных СОМ реализация функций ее ПАК осуществляется с использованием элементов искусственного интеллекта.

Данные об условиях и результатах функционирования ПАК и подсистем СОМ, во-первых, фиксируются и накапливаются в базе знаний, во-вторых, используются для поддержки принятия решений по усилению мер защиты первого уровня САУЗИ (в случае их недостаточности) за счет соответствующих мер второго уровня или ослаблению (в случае избыточности) за счет исключения некоторых мер из состава принятых на первом уровне, в-третьих, применяются для обучения и перепрограммирования других ПАК в составах САУЗИ первого и второго уровней с целью повышения эффективности их функционирования с учетом изменяющихся условий и факторов. Однако решение об усилении или ослаблении мер защиты, а также об изменении условий и режимов функционирования принимается в центре управления САУЗИ.

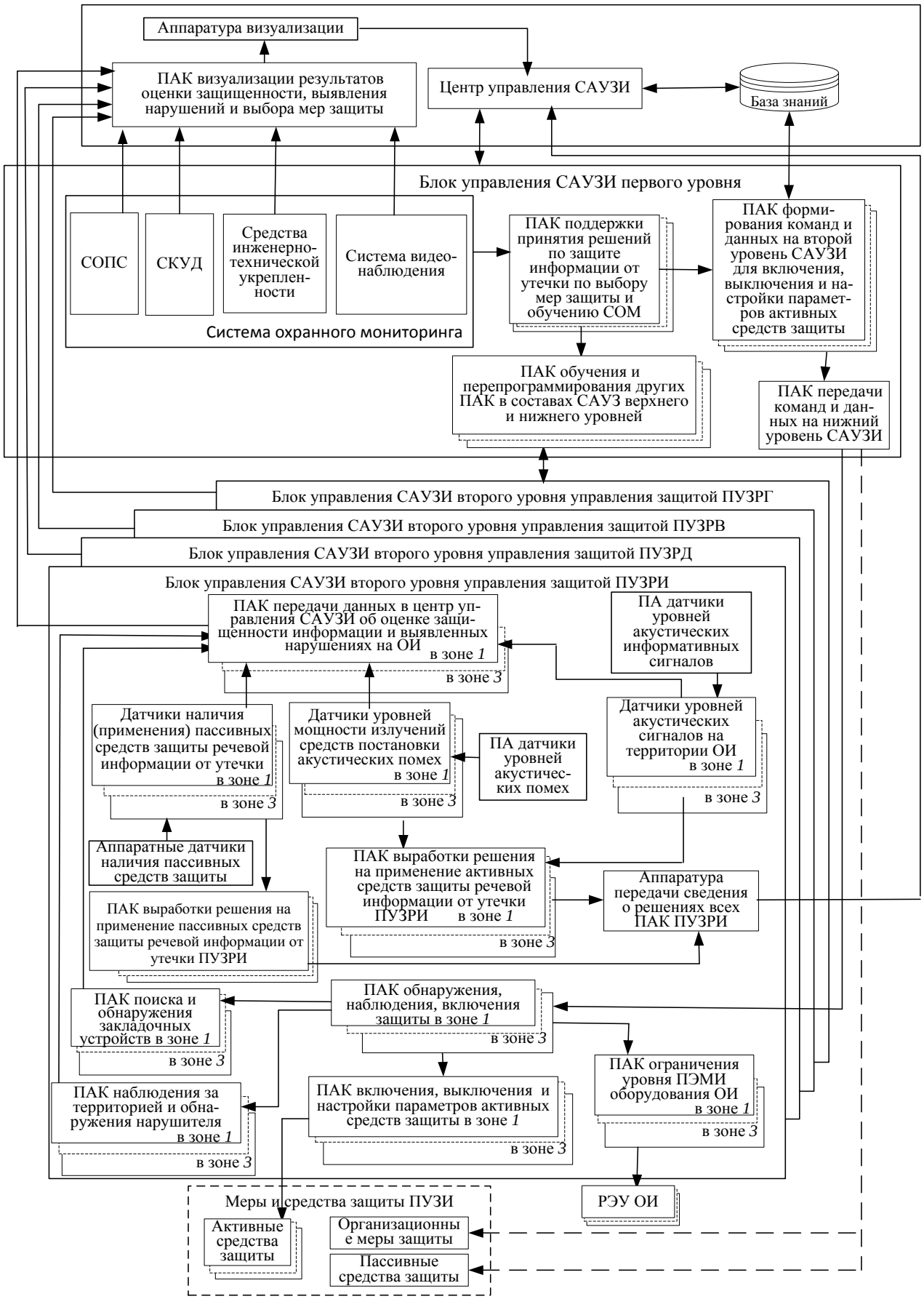

Рис. 3. Пример структуры и состава системы адаптивного управления защитой информации от утечки по техническим каналам на этапе создания ИСЗИ

В частности, на основании решения об усилении или ослаблении мер защиты могут быть сформированы команды и данные для включения и настройки параметров дополнительных пассивных и / или активных средств защиты второго уровня или их выключения. Контроль выполнения этих команд осуществляется ПАК второго уровня управления САУЗИ.

На втором уровне в интересах управления применением технических средств защиты информации пассивного и активного характера в зависимости от видов обрабатываемой информации формируется несколько подсистем (блоков) управления защитой: подсистемы управления защитой речевой (ПУЗРИ), документальной (ПУЗДИ), графической (ПУЗГИ), видовой (ПУЗВИ) информации и др.

Наличие множества условий и факторов, рассмотренных выше, обусловливает необходимость обработки достаточно больших объемов данных, характеризующих состояние объектов защиты, угроз утечки обрабатываемой информации и применяемых мер защиты с учетом изменения их состава в различных зонах защиты, соответствующих рубежам охраны СОМ. Построение такого рода подсистем возможно с использованием ПАК на основе искусственного интеллекта. При этом все подсистемы управления защитой являются объектами управления со стороны центра управления САУЗИ как субъекта управления.

Усиление защиты информации в каждом блоке осуществляется за счет применения, во-первых, дополнительных пассивных технических мер защиты, например, мобильных акустических экранов, штор – жалюзи в оконных проемах и др., во-вторых, организационно-технических мер на основе ПАК наблюдения за территорией и обнаружения нарушителя в зонах *1*, *2* и *3*, в-третьих, технических мер активной защиты, например, генераторов акустического и электромагнитного шума, виброакустических датчиков, ПАК поиска и обнаружения закладочных устройств в зонах и др. При этом решение об усилении / ослаблении защиты за счет организационно-технических и технических мер защиты второго уровня принимается центром управления САУЗИ.

Приоритетными являются, во-первых, меры, реализуемые с использованием ПАК поиска и обнаружения закладочных устройств в соответствующих зонах, во-вторых, пассивные технические меры защиты, управление которыми осуществляется на основании анализа сведений, поступающих от программно-аппаратных (ПА) датчиков их наличия, с использованием ПАК выработки решения на применение. Кроме того, в период реализации информационных процессов по обработке информации на различных этапах создания ИСЗИ может осуществляться наблюдение за территорией с целью своевременного обнаружения нарушителя в зонах *1–3* с использованием соответствующих ПАК.

Данные о результатах реализации этих мер обрабатываются и передаются в центр управления САУЗИ с отображением этих результатов при помощи ПАК визуализации. В случае их недостаточности применяются активные технические средства защиты, управление которыми осуществляется при помощи ПАК выработки решения на применение активных средств защиты информации в составе блока управления САУЗИ соответствующей подсистемы управления защитой.

Циклы управления защитой на первом и втором уровнях управления в существенной степени отличаются, во-первых, составом объектов управления, во-вторых, средствами сбора и обработки информации об их состоянии в условиях динамики управления, в-третьих, характеристиками управляющих воздействий, в-четвертых, средствами исполнения и контроля принятых решений.

На рис. 4 и 5 приведены блок-схемы циклов управления САУЗИ первого и второго уровней, соответствующие приведенным выше их описаниям.

В соответствии с блок-схемой (см. рис. 4) превентивное (предварительное) выявление угроз утечки информации осуществляется путем контроля за появлением нарушителей в зонах *1–3* охраны СОМ [16]. При этом реализуются методы ограничения физического доступа к материальным носителям информации, обрабатываемой в интересах создания ИСЗИ, и оборудованию, используемому для ее обработки.

Оценка защищенности информации от утечки в условиях динамики реализации угроз может быть реализована на основе показателей, учитывающих сценарии выполнения нарушителем действий по перехвату информации в различных условиях обстановки, обусловленных характеристиками зон *1–3* и контролируемых средствами СОМ, предложенных в [4].

Форма представления показателя оценки угрозы утечки информации зависит от сценариев ее реализации нарушителем. Так, в случае, когда нарушитель внутренний и имеет возможность находиться в зоне возможного перехвата информации постоянно, например, при его включении в состав подразделения, выполняющего соответствующие работы в течение *k*-го процесса $k=\overline{1,K}$ на этапе e_j, в качестве такого показателя, по аналогии с [5], будем использовать вероятность $P_1^{\text{o}}(t)$ перехвата хотя бы одного сообщения, содержащего сведения, представляющие интерес для этого нарушителя, за заданное время в условиях отсутствия мер защиты, которая при экспоненциальном приближении рассчитывается по формуле

$$P_1^{\text{o}}(t)=1-\exp\left(-\bar{\mu}^{vm}\cdot p_i^{vm}\cdot t\right), \qquad (4)$$

где $\bar{\mu}^{vm}$ – средняя интенсивность речевых сообщений в составе информационного процесса $I\,\text{Pr}_{e_{jk}}^{vm}$; p_i^{vm} – вероятность того, что в *i*-м речевом сообщении процесса $I\,\text{Pr}_{e_{jk}}^{vm}$ содержатся сведения, представляющие интерес для нарушителя.

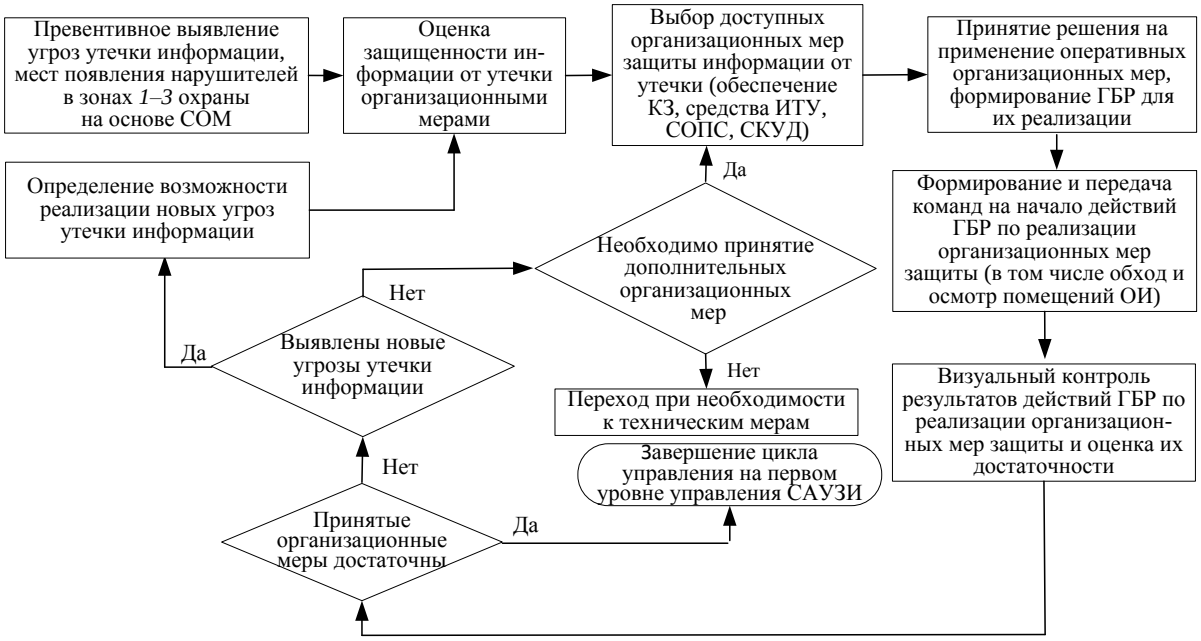

Рис. 4. Блок-схема цикла управления САУЗИ первого уровня

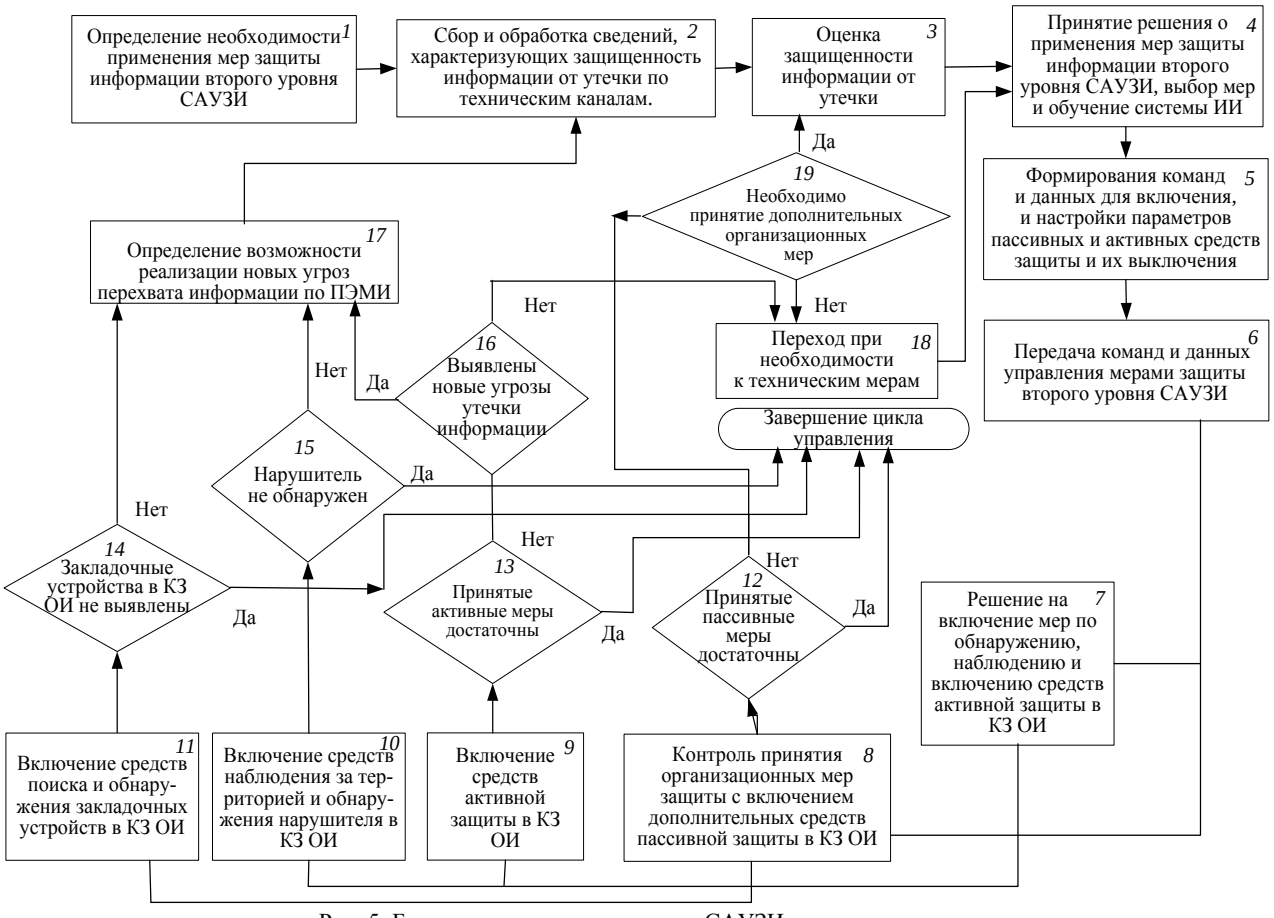

Рис. 5. Блок-схема цикла управления САУЗИ второго уровня

Сценарии постоянного нахождения в зоне возможного перехвата информации могут быть реализованы как внутренним, так и внешним нарушителями различными способами, например, при включении внутреннего нарушителя в состав подразделения, выполняющего работы по созданию ИСЗИ, или путем установки им закладочных устройств в помещениях, в которых выполняются указанные работы, и др., а также в случаях применения внешним нарушителем ТСП за пределами КЗ ОИ, когда размеры такой зоны не соответствуют требованиям о защите информации от утечки и условие (1) не выполняется.

При этом в условиях отсутствия мер защиты вероятность утечки информации фактически зависит от содержания в составе перехваченных сообщений сведений, представляющих интерес для нарушителя.

Усиление мер защиты возможно как за счет применения средств контроля и управления доступом в пределах КЗ ОИ, дополнительно установленных систем видеонаблюдения за пространством в этой зоне или за территорией, к ней прилегающей, а также путем выявления портативных электронных устройств негласного перехвата обрабатываемой информации.

Если нарушитель имеет возможность лишь периодически применять ТСП в зоне возможного перехвата информации, обрабатываемой в интересах создания ИСЗИ (см. рис. 2, *б*), необходимо учитывать поток событий, описываемый средней интенсивностью $\bar{\mu}^{\text{ТСП}}$ применения этого ТСП и средней длительностью $\bar{\tau}\left(u_l^{vm}\right)$ реализации попыток перехвата. Тогда возможность перехвата одного сообщения при отсутствии мер защиты будет определяться вероятностью совпадения этих потоков [5]

$$P_1^0(t)=1-\exp\left[-\bar{\mu}^{vm}\cdot\bar{\mu}^{\text{ТСП}}\left(\bar{\tau}\left(м_i^{vm}\right)+\bar{\tau}\left(u_l^{vm}\right)\right)\right]p_i^{vm}\cdot t\,. \quad (5)$$

В этих условиях усиление мер защиты может быть достигнуто путем применения организационно-технических мероприятий, направленных на снижение интенсивности и продолжительности применения ТСП в случае нарушения условия (1), а также за счет включения технических средств пассивного и активного характера [11].

На втором уровне целью управления (блок *1*) является усиление мер защиты, реализованных на основе СОМ на первом уровне. Сбор и обработка сведений, характеризующих защищенность информации от утечки по техническим каналам, осуществляется с использованием ПА датчиков различной физической природы в составе соответствующих подсистем управления защитой. Для поддержки принятия решений на применение указанных мер в динамике их реализации необходимо создание специализированного ПАК, реализующего указанные меры (блоки *4–17*) в соответствии с описанием второго уровня управления САУЗИ, приведенным выше. ПАК при этом является объектом управления со стороны центра как субъекта управления.

Рассмотренный подход позволяет реализовать поэтапное формирование СЗИ путем усиления мер защиты, применяемых в составе СОМ, управляемых на первом уровне САУЗИ, дополнительными организационно-техническими и техническими мерами, включаемыми на втором уровне САУЗИ.

С учетом динамики параллельно реализуемых процессов обработки защищаемой информации, угроз ее утечки по техническим каналам и защиты от утечки элементы САУЗИ, реализующие оперативное управление техническими средствами защиты, как пассивного, так и активного характера, могут функционировать параллельно друг другу и / или последовательно, в зависимости от множества логических условий. Для оценки эффективности защиты и эффективности управления ею необходимы соответствующие показатели, учитывающие фактор времени и наличие указанных условий, а также модели для расчета этих показателей. Как показано в [5], для моделирования такого рода процессов целесообразно использовать аппарат составных сетей Петри–Маркова. Разработка этих моделей является предметом дальнейших исследований авторов.

Заключение

1. Возможное получение нарушителем доступа к содержанию информации, используемой в интересах создания ИСЗИ на этапах, предшествующих ее эксплуатации, может использоваться нарушителем для реализации УБИ, обрабатываемой на этапе эксплуатации этой ИСЗИ. При этом в качестве негативного последствия реализации УБИ в процессе создания ИСЗИ рассматривается утечка информации, обрабатываемой на каждом из этапов. При организации и обеспечении защиты этой информации от утечки необходимо учитывать изменения форм ее представления, условий динамики ее обработки, совокупность условий и факторов, создающих опасность реализации угроз утечки по техническим каналам. Указанные изменения могут быть учтены путем управления защитой на основе САУЗИ, создаваемой по централизованному принципу и обеспечивающей управление на двух уровнях путем усиления мер защиты в соответствии с изменяющимися условиями обстановки.

2. Обоснованы возможности применения существующего аппарата теории управления в интересах создания САУЗИ от утечки по техническим каналам на ОИ в условиях изменения состава объекта защиты, внутренних и внешних факторов, характеризующих динамику функционирования такой САУЗИ, а также обоснования направлений решения проблемных вопросов оценки эффективности такого рода системы и эффективности управления ею.

3. Проблемные вопросы, возникающие при создании САУЗИ, связаны, во-первых, с изменениями видов информации, обрабатываемой на различных этапах создания ИСЗИ как объекта защиты, во-вторых, с описанием динамики параллельно реализуемых процессов обработки этой информации, условий и факторов реализации угроз ее утечки по техническим каналам и защиты от утечки, в-третьих, с оценкой эффективности защиты и эффективности управления защитой.

4. Для оценки эффективности управления защитой информации на основе САУЗИ на этапах создания ИСЗИ необходимо соответствующее методическое обеспечение управления защитой. Его создание связано с вопросами обоснования показателей и разработки математических моделей для их расчета с учетом фактора времени и различных логических условий управления защитой информации от утечки по ТКУИ, включающих алгоритмы оценки обстановки на ОИ, в составе которого создается ИСЗИ, и на территории, прилегающей к объекту, а также совокупность возможных алгоритмов выбора целесооб-

разного состава мер защиты в САУЗИ, учитывающих указанные условия.

5. Для оценки эффективности управления защитой информации от утечки на основе САУЗИ предложено использовать количественные показатели, позволяющие определить влияние управления защитой на ее эффективность. Для расчета таких показателей с учетом фактора времени и логических условий, определяющих динамику реализации исследуемых процессов, целесообразно использовать аппарат составных сетей Петри–Маркова. Разработка этих моделей является предметом дальнейших исследований авторов. В качестве основы для формирования графов такого рода сетей могут использоваться разработанные блок-схемы циклов управления САУЗИ для двух уровней.

Литература

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 [Электронный ресурс]. – Режим доступа: https://base.garant.ru/ 70391358, свободный (дата обращения: 22.12.2024).

2. ГОСТ Р 51583. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – М.: Стандартинформ, 2014. – 15 с.

3. ГОСТ 34.601–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы: стадии создания. – М.: Стандартинформ, 2009. – 6 с.

4. Авсентьев О.С. Модели обоснования организационно-технического обеспечения мероприятий по созданию СЗИ объектов информатизации / О.С. Авсентьев, В.В. Бутов, А.Г. Вальде // Труды учебных заведений связи. – 2024. – Т. 10, № 5. – С. 93–108. DOI 10.31854/1813-324X-2024-10-5-92-107.

5. 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. – P. 46–62.

6. Ожиганова М.И. Построение адаптивных систем защиты информации / М.И. Ожиганова, А.О. Калита, Е.Н. Тищенко // НБИ технологии. – 2019. – Т. 13, № 4. – С. 12–21. DOI: 10.15688/NBIT.jvolsu.2019.4.2.

7. Жмурко Д.Ю. Понятие, сущность и классификация адаптивного управления системами с организационной сложностью // Научный журнал КубГАУ. – 2013. – № 90 (06) [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/ponyatie-suschnost-i-klassifikatsiya-adaptivnogo-upravleniya-sistemami-s-organizatsionnoy-slozhnostyu/viewer, свободный (дата обращения: 20.12.2024).

8. Большой энциклопедический словарь. – 2-е изд., перераб. и доп. – М.: Большая Российская энциклопедия; СПб.: Норинт, 2002. – 1456 с.

9. Методика оценки угроз безопасности информации: метод. документ. – Утв. ФСТЭК России 05 февраля 2021 г. – М.: ФСТЭК, 2021. – 83 с.

10. Язов Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. – СПб.: Наукоемкие технологии, 2023. – 258 с.

11.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, свободный (дата обращения: 25.12.2024).

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

13. Коршунов Ю.М. Математические основы кибернетики: учеб. пособие для вузов. – 2-е изд., перераб. и доп. – М.: Энергия, 1980. – 424 с.

14. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 8 с.

15. Зарубин В.С. Системы охранной безопасности: учеб. пособие / В.С. Зарубин и др. – Воронеж: Воронежский институт МВД России, 2012. – 282 с.

16. Язов Ю.К. Проблемные вопросы управления защитой информации от утечки по техническим каналам с применением многоагентных систем / Ю.К. Язов, А.О. Авсентьев // Вопросы кибербезопасности. – 2024. – № 6 (64). – С. 85–97. DOI: 10.21681/2311-3456-2024-Z-XX-YY.

Авсентьев Олег Сергеевич
Д-р техн. наук, проф. каф. информационной безопасности Воронежского института МВД России
Патриотов пр., 53, г. Воронеж, Россия, 394065
Тел.: +7 (473-2) 64-52-44.
Эл. почта: osaos@mail.ru

Томилова Эльвира Александровна
Адъюнкт Воронежского института МВД России.
Патриотов пр., 53, г. Воронеж, Россия, 394065
Тел.: +7-904-531-35-34.
Эл. почта: tomilovaea09@gmail.com

Avsentiev O.S., Tomilova E.A.

Adaptive Information Security Management Models in the Process of Developing a State Information System

The article considers problematic issues of developing adaptive control models for information security in a state information system during the creation of its security system. These models aim to take into account changes in the representation formats of protected information, the dynamic conditions of its processing, and factors posing a threat of leakage through technical channels. Descriptive models of the investigated processes have been developed. Feasibility of considering these changes and conditions is substantiated through an adaptive information security management system established on a centralized principle, providing two-level control by reinforcing security measures in accordance with changes in the composition of the protected object, internal and external factors characterizing the dynamics of the system's operation, and approaches to address-

ing problematic issues in assessing its effectiveness. To calculate performance evaluation metrics for information security management during the stages of creating a secure information system, considering the time factor and various logical control conditions, the application of composite Petri-Markov nets is proposed. Control cycle flowcharts for two levels has been developed, which are considered as the basis for constructing composite Petri-Markov net graphs.

Keywords: secure information system, adaptive information security management system, information leakage threat, conditions and factors, effectiveness of information security management.

DOI: 10.21293/1818-0442-2024-27-4-61-73

References

1. *On the approval of requirements for protecting non-state secret information in state information systems* [Electronic resource]. FSTEC order of Russia dated 11 February 2013, no. 17. Available at: https://base.garant.ru/70391358, free (Accessed: 22.12.2024) (in Russ.).

2. GOST P 51583. [Information security. Procedure for creating automated systems in a secure configuration. General provisions]. M., Standartinform, 2014, 15 p. (in Russ.).

3. GOST 34.601–90. [Information technology. Set of standards for automated systems. Automated systems: stages of creation]. M., Standartinform, 2009, 6 p. (in Russ.).

4. Avsentiev O.S., Butov V.V., Valde A.G. [Models for justifying organizational and technical support for measures to create SIS informatization objects]. *Works of communication institutions*. 2024, vol. 10, no. 5, pp. 93–108. DOI: 10.31854/1813-324X-2024-10-5-92-107 (in Russ.).

5. 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 State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS)*, 2021, vol. 14, no. 4, pp. 46–62.

6. Ozhiganova M.I., Kalyta A.O., Tishchenko E.N. [Construction of adaptive information security systems]. *NBI technology.* 2019, vol. 13, no. 4, pp. 12–21. DOI: 10.15688/NBIT.jvolsu.2019.4.2 (in Russ.).

7. Zhmurko D.Ju. [Concept, essence and classification of adaptive management systems with organizational complexity]. *Scientific journal of KubaGAU,* 2013, no. 90 (06) [Electronic resource]. Available at: https://cyberleninka.ru/ article/n/ponyatie-suschnost-i-klassifikatsiya-adaptivnogo-upravleniya-sistemami-s-organizatsionnoy-slozhnostyu/viewer, free (Accessed: December 20.12.2024) (in Russ.).

8. *The Grand Encyclopaedic Dictionary*. 2nd ed., rev. and exp. M.: The Great Russian Encyclopedia; SPb.: Norinth, 2002, 1456 (in Russ.).

9. *Guidance document. Methodology for assessing information security threats.* Approved by CCFTU Russia 5 February 2021 (in Russ.).

10. Yazov Y.Q., Solovyev S.V. *Methodology for evaluating effectiveness of information protection in information systems from unauthorized access: monograph*. Saint-Petersburg: Science-intensive technologies, 2023, 258 p. (in Russ.).

11. *Special requirements and recommendations for the technical protection of confidential information (TPC-K), Approved by Order of the State Technical Commission of Russia dated 30.08.2002* no. 282 [Electronic resource]. Available at: http://www.rfcmd.ru/ sphider/docs/InfoSec/ RD_FSTEK, free (Accessed: 25.12.2024) (in Russ.).

12. Avsentiev A.O., Ponomarenko S.V., Rojkov A.G. Verbal model of the technical channel for information leakage due to side electromagnetic radiation at the data processing facilities. *Bulletin of the Voronezh Institute of the FSIN of Russia*. 2020, no. 1, pp. 9–21 (in Russ.).

13. Korshunov Y.M. *Mathematical foundations of cybernetics: study, a manual for universities*. 2nd ed., rev. and exp. M.: Energy, 1980, 424 p. (in Russ.).

14. GOST R 50922–2006. [Information protection. Basic terms and definitions]. M., Standartinform, 2008. 8 p. (in Russ.).

15. Zabrutin V.S. et al. *Security System*: Training manual. Voronezh, Voronezh Institute of the Ministry of Internal Affairs of Russia, 2012. 282 p. (in Russ.).

16. Yazov Y.K., Avsentiev A.O. Problematic issues of management of information protection against leakage through technical channels using multi-agent systems. *Cybersecurity*, 2024, no. 6 (64), pp. 85–97. DOI: 10.21681/2311-3456-2024-Z-XX-YY (in Russ.).

Oleg S. Avsentiev
Doctor of Technical Sciences, Professor of the Information security department, Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation
53, Patriotov pr., Voronezh, Russia, 394065
Phone: +7 (473-2) 64-52-44.
Email: osaos@mail.ru

Elvira A. Tomilova
PhD student, Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation
53, Patriotov pr., Voronezh, Russia, 394065
Phone: +7-904-531-35-34.
Email: tomilovaea09@gmail.com