Научная статья
УДК 004.056:519.1
https://doi.org/10.31854/1813-324X-2024-10-5-92-107

Модели обоснования организационно-технического обеспечения мероприятий по созданию СЗИ объектов информатизации

Олег Сергеевич Авсентьев[1] ✉, osaos@mail.ru
Владислав Вячеславович Бутов[1], butov18@mail.ru
Андрей Геннадьевич Вальде[2], avalde@mvd.ru

[1]Воронежский институт МВД России,
Воронеж, 394065, Российская Федерация
[2]Управление МВД России по Амурской области,
Благовещенск, 675000, Российская Федерация

Аннотация

Актуальность *статьи обусловлена необходимостью защиты информации на всех этапах создания информационной системы при отсутствии соответствующего организационно-технического обеспечения. Для обоснования такого рода обеспечения необходимы математические модели, учитывающие условия и случайный характер реализации во времени разнородных процессов обработки информации на каждом из этапов, угроз ее безопасности и защиты от этих угроз. В статье рассматриваются подходы к разработке таких моделей на основе аппаратов теории потоков и теории составных сетей Петри – Маркова, возможности применения которых для моделирования исследуемых процессов ранее не рассматривались.*

Цель статьи. *Раскрыть содержание вопросов, связанных с обоснованием организационно-технического обеспечения защиты информации на этапах создания информационной системы, показать необходимость и пути количественной оценки угроз ее безопасности и защищенности от этих угроз. Для этого были применены* ***методы*** *функционально-структурного анализа, теории вероятностей и теории потоков. В ходе* ***решения*** *научной задачи показана актуальность обоснования организационно-технического обеспечения защиты информации на этапах создания информационных систем, разработаны описательные модели процессов ее обработки, приведены временны́е диаграммы сценариев реализации угроз в условиях отсутствия мер защиты и применения превентивно установленных мер организационно-технического характера, предложены показатели и аналитические соотношения для их расчета.*

Научная новизна *статьи состоит в том, что в ней впервые рассмотрены вопросы организационно-технического обеспечения защиты информации на этапах создания информационной системы, рассмотрены теоретические аспекты количественной оценки угроз ее безопасности и защищенности от этих угроз на основе теории потоков и перспективы применения теории составных сетей Петри – Маркова.*

Значимость (теоретическая). *Установлены условия реализации исследуемых процессов и возможности применения теории потоков и аппарата составных сетей Петри – Маркова для их моделирования.*

Значимость (практическая). *Полученные в работе результаты могут быть использованы при обосновании организационно-технического обеспечения защиты информации на этапах создания информационных систем различных организаций (как государственных, так и негосударственных), для которых реализация угроз на этих этапах может привести к нанесению ущерба их деятельности.*

Ключевые слова: *информация, информационная система, меры защиты информации, организационно-технические меры защиты, система защиты информации, этапы создания системы защиты информации, объекты защиты, теория потоков*

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

Original research
https://doi.org/10.31854/1813-324X-2024-10-5-92-107

Justification Models of Organizational and Technical Support of Measures to Create Information Protection System of Informatization Objects

Oleg S. Avsentyev [1] ✉, osaos@mail.ru
Vladislav V. Butov [1], butov18@mail.ru
Andrei G. Valde [2], avalde@mvd.ru

[1]Voronezh Institute of the Ministry of the Interior of the Russian Federation,
Voronezh, 394065, Russian Federation
[2]Ministry Department of Internal Affairs of Russia in the Amur Region,
Blagoveshchensk, 675000, Russian Federation

Annotation

The relevance *of the article is due to the need to protect information at all stages of creating an information system in the absence of appropriate organizational and technical support. To justify this kind of provision, mathematical models are needed that take into account the conditions and the random nature of the implementation of heterogeneous information processing processes in time at each stage, threats to its security and protection from these threats. The article discusses approaches to the development of such models based on the apparatus of flow theory and the theory of composite Petri –Markov networks, the possibilities of which for modeling the processes under study have not been previously considered.*

The purpose of the article*. To reveal the content of issues related to the justification of organizational and technical support for information protection at the stages of creating an information system, to show the need and ways to quantify threats to its security and protection from these threats. For this purpose, the* ***methods*** *of functional and structural analysis, probability theory and flow theory were applied. In the course* ***of solving*** *the scientific problem, the relevance of substantiating the organizational and technical support of information protection at the stages of creating information systems is shown, descriptive models of its processing processes are developed, time diagrams of threat scenarios are given in the absence of protection measures and in the conditions of using preventive organizational and technical measures, indicators and analytical ratios for their calculation are proposed.* ***The scientific novelty*** *of the article consists in the fact that for the first time it examines the issues of organizational and technical support for information protection at the stages of creating an information system, examines the theoretical aspects of quantifying threats to its security and protection from these threats based on flow theory and prospects for applying the theory of composite Petri-Markov networks.* ***Significance (theoretical)****. The conditions for the implementation of the studied processes and the possibility of applying the theory of flows and the apparatus of composite Petri–Markov networks for their modeling are established.* ***Significance (practical)****. The results obtained in the work can be used to justify the organizational and technical provision of information protection at the stages of creating information systems of various organizations (both state and non-state), for which the implementation of threats at these stages may lead to damage to their activities.*

Keywords: *information, information system, information protection measures, organizational and technical protection measures, information protection system, stages of creating an information protection system, protection objects, flow theory*

For citation: Avsentyev O.S., Butov V.V., Valde A.G. Justification Models of Organizational and Technical Support of Measures to Create Information Protection System of Informatization Objects. *Proceedings of Telecommunication Universities.* 2024;10(5):93–108. (in Russ.) DOI:10.31854/1813-324X-2024-10-5-92-107. EDN:AKWAWD

Введение

Защита информации является составной частью работ по созданию информационной системы (ИС) какой-либо организации как государственной, так и негосударственной, осуществляющей деятельность в соответствии с действующим законодательством России, и обеспечивается на всех стадиях (этапах) создания ИС (приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в ред. Приказов ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106)), приведенных, например, в [1]. При этом сведения, содержащиеся в передаваемых, принимаемых, обрабатываемых сообщениях в интересах создания ИС и ее системы защиты информации (СЗИ) в помещениях объекта информатизации, могут представлять интерес для нарушителей, поскольку они могут использоваться для реализации угроз безопасности информации (УБИ), как обеспечивающего ресурса деятельности организации, в интересах которой в помещении объекта создается ИС, на этапе эксплуатации системы [2]. Возможность реализации УБИ на различных этапах процесса создания ИС на объекте информатизации в условиях отсутствия сформированной СЗИ и нанесения ущерба в отношении как обрабатываемой информации, так и оборудования, используемого для ее обработки, обусловливает необходимость блокирования этих угроз на каждом из этапов. При этом, как отмечено в Методике оценки угроз безопасности информации, утвержденной ФСТЭК России 05 февраля 2021 г., необходимо «систематически» осуществлять оценку УБИ. Однако в Методике отсутствуют обоснования «систематичности», критериев и методик оценки УБИ на различных этапах существования ИС. Следует отметить, что в соответствии с Приказом № 17 и Методикой, разделение на этапы процесса формирования СЗИ при создании ИС в явном виде не предусмотрено, что вызывает определенные трудности такого разделения, а также трудности оценки УБИ и их блокирования мерами защиты информации, обрабатываемой на различных этапах. Применение для этих целей подхода к формированию СЗИ на основе «базового набора мер защиты» (Приказ № 17) невозможно по ряду причин, связанных с неопределенностью относительно класса защищенности, создаваемой ИС (категории объекта информатизации), ее структурно-функциональных характеристик, используемых информационных технологий, особенностей функционирования средств и систем обработки информации, перечня УБИ, в условиях отсутствия разработанной модели угроз.

Указанные обстоятельства порождают противоречие, разрешение которого на основе существующего методического обеспечения реализации рассматриваемых процессов невозможно ни в практическом, ни в теоретическом плане. С точки зрения практики создания СЗИ, защите подлежит не только информация, обрабатываемая в ИС на этапе эксплуатации, но и информация, обрабатываемая на всех предшествующих и последующих этапах существования ИС и объекта в целом.

В качестве объектов защиты рассматриваются:

– территория объектов информатизации;

– здание (сооружение), в пределах которого ИС размещается;

– защищаемое помещение в этом здании;

– информация и / или информационные ресурсы [3].

При этом на различных этапах состав объектов защиты модифицируется [4], что обусловливает необходимость учета, во-первых, изменения условий реализации УБИ при их оценке на различных этапах (невозможно сделать экспертным путем), во-вторых, отсутствия в настоящее время методического и организационно-технического обеспечения мероприятий, проводимых на этих этапах в интересах создания СЗИ системы и объектов информатизации, а также математических моделей, позволяющих проводить оценку угроз, обеспечить защиту и оценить защищенность информации в рассматриваемых условиях.

Теоретические аспекты данного противоречия состоят в следующем. Исследуемые процессы обработки информации, используемой в интересах создания ИС и объекта информатизации, выполнения нарушителем действий по реализации УБИ в отношении этой информации и оборудования для ее обработки, а также процессы реализации мер защиты, направленные на блокирование угроз, во-первых, взаимосвязаны и реализуются как параллельно, так и последовательно, во-вторых, характеризуются случайной последовательностью смены их состояний во времени, а также наличием параллельно выполняемых действий и логических условий, определяющих возможность реализации. Как показано в [5, 6], оценка УБИ в динамике их реализации и защищенности информации в этих условиях возможна на основе применения теории потоков и аппарата составных сетей Петри – Маркова [7, 8]. Однако возможности их применения для моделирования указанных процессов, реализуемых в интересах обеспечения защиты информации на различных этапах создания ИС и объекта информатизации, ранее не рассматривались. Кроме того, отсутствуют модели обоснования методического и организационно-технического обеспечения защиты информации, обрабатываемой при проведении работ на различных этапах создания СЗИ и объекта информатизации.

Указанные обстоятельства обусловливают актуальность материала данной статьи, посвященной обоснованию такого рода методического и организационно-технического обеспечения мероприятий по защите информации, обрабатываемой в интересах создания ИС и СЗИ на объекте информатизации, показателей для оценки УБИ и ее защищенности от угроз, а также разработке моделей для расчета этих показателей.

1. Описание информации, используемой на различных этапах создания СЗИ на объекте информатизации

Процесс создания ИС представляет собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполняемых в интересах создания ИС, соответствующей заданным требованиям, и осуществляется во всех организациях, участвующих в процессе создания этих систем, в том числе и в организации, выступающей в качестве заказчика [1, 9]. В целях рационального планирования и организации этих работ реализуются информационные процессы по обработке сведений в различных формах их представления. Однако при этом в [1] не предполагается проведение работ по защите информации, в том числе на этапе эксплуатации ИС.

В соответствии с существующим методическим подходом, защита информации осуществляется на всех этапах создания ИС применительно к конкретному объекту защиты с учетом:

– видов обрабатываемой информации и ее материальных носителей;

– структурно-функциональных характеристик создаваемой ИС;

– выявленных уязвимостей в ее составе;

– факторов, влияющих на безопасность как информации, так и оборудования, используемого для ее обработки, которые могут быть применены нарушителем для реализации УБИ (Приказ № 17).

С учетом данного подхода, в [4] предложено разделение процесса создания СЗИ на 6 этапов, соответствующих перечню мероприятий по защите информации, обрабатываемой в процессе реализации этих этапов (Приказ № 17):

$$E = \langle e_i, i = \overline{1,6} \rangle, \quad (1)$$

где e_1 = ⟨формирование требований к защите информации⟩; e_2 = ⟨формирование СЗИ⟩; e_3 = ⟨внедрение СЗИ⟩; e_4 = ⟨аттестация ОИ по требованиям защиты информации⟩; e_5 = ⟨обеспечение защиты информации в ходе эксплуатации объекта информатизации⟩; e_6 = ⟨обеспечение защиты информации в ходе вывода из эксплуатации аттестованного объекта информатизации⟩.

При этом на этапах e_5 и e_6 защита информации осуществляется на основе уже сформированной и аттестованной СЗИ по требованиям к защите, а на этапах $e_1 \div e_4$ выполняются работы, при выполнении которых обрабатывается информация в различных формах ее представления в условиях отсутствия сформированной СЗИ. Часть работ на этапах $e_1 \div e_4$ производится сторонними организациями (разработчик ИС и ее СЗИ; изготовитель и поставщик технических и программных средств), имеющими лицензию на выполнении соответствующих видов деятельности с обеспечением необходимых мер защиты информации, обрабатываемой в процессе ее реализации. В связи с этим в данной статье указанные меры не рассматриваются. Однако комплекс работ по формированию требований к СЗИ ИС, ее разработке (проектированию), внедрению, аттестации на соответствие требованиям безопасности информации и ввод в действие в соответствии с Приказом № 17 [9] осуществляется обладателем информации (заказчиком) в условиях отсутствия сформированной СЗИ, соответствующей требованиям о безопасности информации.

На рисунке 1 представлена обобщенная схема, отражающая цели выполнения работ и их последовательность на этих этапах, где ЗИ – защита информации; ОИ – объект информатизации; НСД – несанкционированный доступ.

Каждый из этапов схемы (см. рисунок 1), в свою очередь, разделяется на процессы, соответствующие целям выполняемых работ:

$$e_1 = \langle e_{11} \div e_{15} \rangle,\ e_2 = \langle e_{21} \div e_{23} \rangle,$$
$$e_3 = \langle e_{31} \div e_{33} \rangle,\ \ e_4 = \langle e_{41} \rangle.$$

Для обеспечения защиты информации и оборудования ИС в составе объекта информатизации, в соответствии с Приказом № 17, руководителем организации назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации в части:

– разработки задания на создание ИС и ее СЗИ (этап e_1);

– включения в документацию на ИС обоснованных требований о защите обрабатываемой информации и контроля их выполнения в процессе экспертизы документации (этап e_2);

– испытаний и приемки как ИС в целом, так и ее СЗИ (этап e_3);

– организации аттестации ИС на соответствие требованиям безопасности информации (этап e_4);

– сопровождения ИС в ходе ее эксплуатации [9].

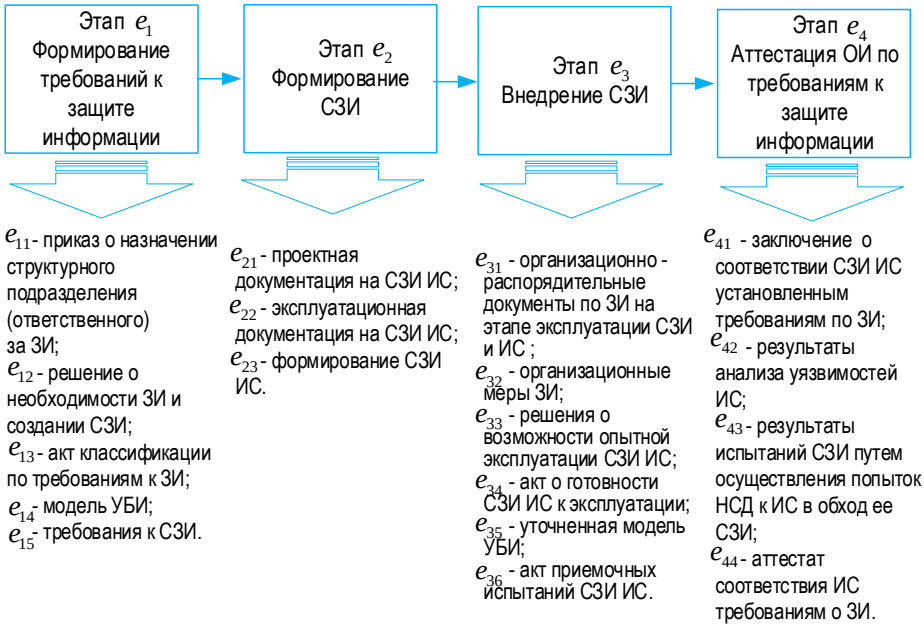

Рис. 1. Цели и последовательность выполнения работ на этапах $e_1 \div e_4$ создания ИС в условиях отсутствия сформированной СЗИ

Fig. 1. Objectives and Sequence of Work at Stages $e_1 \div e_4$ of Creating an Information System in the Absence of a Formed Information Security System

Как правило, состав и функции лиц, включенных в данное подразделение, определяются соответствующим приказом по организации. При его создании и доведении до исполнителей реализуется процесс обработки информации (e_{11}) как в речевой форме, так и форме документа на бумажном и / или электронном носителе. За счет нарушения конфиденциальности сведений, содержащихся в приказе, могут быть раскрыты, во-первых, цель и задачи создания ИС и ее СЗИ, а также направления деятельности организации, в интересах которой ИС создается, во-вторых, сведения о лицах, допущенных к информационным ресурсам организации, используемым в процессе выполнения работ на различных этапах существования, в том числе, на этапе эксплуатации ИС и ее СЗИ.

Процесс e_{12} реализуется в интересах принятия решения о необходимости защиты информации на основе:

– сведений о видах деятельности, реализуемых в организации, о самом объекте информатизации, в составе которого планируется создание ИС;

– выявления проблем, связанных с обеспечением эффективности деятельности, решение которых возможно за счет создания ИС;

– оценки (правовой, технико-экономической, социальной и т. п.) целесообразности создания ИС и ее СЗИ.

Нарушение конфиденциальности информации, содержащей такого рода сведения, может быть использовано нарушителем при разработке сценариев реализации УБИ в отношении как этих сведений, так и информации, обрабатываемой на этапе эксплуатации ИС, учитывающих уровень защиты информации на основе создаваемой СЗИ. Сценарии реализации УБИ могут быть скорректированы нарушителем для соответствующих способов их реализации применительно к конкретным объектам воздействия, последовательности выполняемых действий, привлечения необходимых сил и средств, соответствующих его возможностям (потенциалу), а также доступности различных способов реализации УБИ.

Определение класса защищенности ИС (категория объекта информатизации) определяется при реализации процесса e_{13} на основе оценки важности информации, обрабатываемой в ИС в интересах обеспечения деятельности организации и масштаба создаваемой ИС. Важность информации определяется величиной ущерба, связанного с нарушением свойств информации актуальных для организации, в интересах которой создается ИС. При наличии сведений о важности информации нарушитель имеет возможность планирования выделяемых ресурсов для реализации угроз в отношении этой информации и оборудования ИС.

В соответствии с Приказом № 17 и Методикой, процесс e_{14} разработки модели УБИ содержит исходные данные для описания ИС и ее структурно-функциональных характеристик, а также описания возможностей нарушителей (модель нарушителя), уязвимостей ИС, способов реализации угроз и последствий от нарушения свойств безопасности информации.

В связи с тем, что обработка информации, используемой в интересах создания ИС и ее СЗИ, осуществляется, как правило, в помещениях объекта информатизации, то в качестве УБИ целесообразно рассматривать:

1) угрозы, связанные с несанкционированным доступом к информации и оборудованию, используемому для ее обработки на различных этапах;

2) угрозы утечки этой информации по техническим каналам.

В соответствии с Приказом № 17 в общем случае к основным элементам описания УБИ относятся:

– источник угрозы (нарушитель);

– уязвимости системного и прикладного программного обеспечения ИС (в случае использования для обработки информации в компьютерных системах);

– факторы, воздействующие на безопасность информации (при исследовании возможностей ее утечки по техническим каналам), используемые нарушителем для реализации угроз;

– способы реализации угроз и сценарии несанкционированных действий, выполняемых в соответствии с Методикой в ходе их реализации [10].

С целью выполнения требований о «систематической» оценке УБИ для разработки модели угроз, актуальных для соответствующего этапа создания СЗИ, целесообразно воспользоваться программой, разработанной в интересах автоматизации процесса формирования перечня угроз специалистами ФСТЭК России и представленной в разделе официального сайта «БДУ – формирование перечня угроз» (https://bdu.fstec.ru/threat-section/shaper-threats). Однако для проведения оценки необходимо решать ряд задач из их перечня, приведенного в Методике, решение которых невозможно на основе данной программы. К таким задачам относятся: оценка возможности реализации УБИ и определение их актуальности; оценка сценариев реализации УБИ в ИС. В условиях изменений состава объектов защиты при выполнении различных работ на этапах создания СЗИ изменяются и условия для решения этих задач, что затрудняет своевременную выработку адекватных и эффективных мер по защите информации на каждом из этапов.

В процессе оценки УБИ, в соответствии с Методикой, ответственными работниками (далее – работники подразделения) организации используются различные исходные данные, включающие общедоступные сведения, факты использования которых могут быть применены нарушителем для реализации УБИ, обрабатываемой на этапе эксплуатации созданной ИС и ее СЗИ. Так, при использовании программы (https://bdu.fstec.ru/threat-section/shaper-threats) сведения о выборе негативных последствий от реализации угроз могут быть применены нарушителем для раскрытия цели и задач обеспечения защиты информации в ИС и на объекте информатизации, а также для определения актуальных угроз из их общего перечня, реализация которых может причинить ущерб обеспечению деятельности организации. На основе перечня актуальных УБИ и последующего выбора объектов их воздействия, могут быть раскрыты сведения о структуре создаваемой ИС, ее СЗИ и их функциях. Результаты последующего выбора компонентов объектов воздействия могут быть использованы нарушителем для определения способов реализации угроз, например, компьютерных атак на ИС, или угроз утечки информации по техническим каналам. В соответствии с Методикой на основе сведений, используемых на перечисленных этапах формирования модели угроз, нарушитель (внутренний или внешний) может оценить свои возможности (потенциал нарушителей – отдельных физических лиц, организованных преступных групп, организаций – конкурентов, спецслужб иностранных государств и т. п.) по их реализации, а также определить перспективы их повышения, например, путем сговора внешних и внутренних нарушителей.

Формирование требований к СЗИ осуществляется в процессе e_{15} с учетом класса защищенности ИС и разработанной модели угроз. Эти требования, в соответствии с Приказом № 17, включаются в частное техническое задание на создание СЗИ и также содержат сведения, которые могут быть использованы нарушителем при реализации УБИ, обрабатываемой в ИС на этапе ее эксплуатации, в интересах обхода применяемых мер защиты информации и с учетом положений политик обеспечения информационной безопасности организации.

На этапе e_2 работниками подразделения осуществляется контроль проведения разработчиком работ по проектированию (процесс e_{21}), формированию эксплуатационной документации (процесс e_{22}) на СЗИ и непосредственно созданию СЗИ ИС (процесс e_{23}).

В процессе e_{21} лицами, осуществляющими контроль за проектированием, путем обсуждения на совещании рабочей группы рассматриваются состав пользователей, процессов и других субъектов доступа, объектов, подлежащих защите в составе ИС и объектов информатизации, правила разграничения, методы контроля и управления доступом. В соответствии с техническим заданием и требованиями, разработанными в процессе e_{15}, осуществляется согласование мер защиты информации, включаемых разработчиком в состав СЗИ, структуры и размещения ее элементов в составе объекта информатизации с учетом наличия у применяемых для реализации этих мер средств защиты сертификатов на соответствие требованиям по безопасности информации, их соответствия определенному

классу защищенности (процесс e_{13}) ИС, и других параметров СЗИ, определенных в Приказе № 17, осуществляется обсуждение возможных уязвимостей ИС, которые могут привести к возникновению УБИ. В результате реализации угроз утечки речевой информации при выполнении работ в процессе e_{21} нарушителем могут быть раскрыты сведения о СЗИ, режимах ее функционирования и т. п., которые могут быть использованы на этапе эксплуатации ИС и объекта информатизации с целью обхода СЗИ в интересах реализации УБИ. Результаты проектирования СЗИ отражаются в проектной документации на ИС, оформленных на бумажных и электронных носителях.

В процессе e_{22} рассматривается разрабатываемая эксплуатационная документация на СЗИ, включающая документы, содержащие описания: структуры СЗИ; мест размещения элементов этой структуры в помещении объекта информатизации; настроек их программного обеспечения и параметров функционирования мер и средств защиты информации в составе СЗИ; правил эксплуатации СЗИ ИС.

В процессе e_{23} работниками подразделения рассматриваются результаты работ по формированию СЗИ по ее макетированию и тестированию:

– проверка работоспособности средств защиты информации в составе СЗИ и выполнением требований к СЗИ ИС, содержащихся в составе технического задания (процесс e_{15});

– корректировка принятых проектных решений (процесс e_{21}); при этом возможно применение методов моделирования ИС на основе средств вычислительной техники.

Неисполнение конфиденциальности информации о сформированной СЗИ раскрывает сведения, которые могут быть использованы нарушителем для обхода мер защиты при реализации УБИ на этапе эксплуатации ИС и объекта информатизации в целом.

На этапе e_3 при внедрении СЗИ работниками подразделения рассматриваются результаты работ, проводимых разработчиком, в соответствии с проектной (e_{21}) и эксплуатационной (e_{22}) документацией, включающих:

– установку и настройку средств защиты информации в составе СЗИ с учетом корректировки состава ее структуры (e_{23});

– разработку организационно-распорядительных документов по защите информации на этапе эксплуатации СЗИ и ИС объектов информатизации (процесс e_{31});

– внедрение организационных мер защиты информации (процесс e_{32});

– предварительные испытания и опытную эксплуатацию СЗИ (процессы e_{33} и e_{34});

– анализ уязвимостей ИС, уточнение модели УБИ и принятие (дополнение) мер защиты информации по их блокированию (процесс e_{35});

– приемочные испытания СЗИ (процесс e_{36}).

При выполнении работ в процессе e_{31} в речевой форме обсуждаются вопросы, связанные: с управлением создаваемой СЗИ и реагированием на выявленные инциденты, которые могут привести к возникновению УБИ и нарушению функционирования оборудования ИС; с управлением конфигурацией и контролем защищенности информации, содержащейся в ИС, после аттестационных испытаний, а также с обеспечением защиты информации на этапе вывода ИС из эксплуатации. Раскрытие этих сведений позволит нарушителю на этапе эксплуатации СЗИ разрабатывать сценарии реализации УБИ, в том числе с учетом обхода дополненных мер защиты в составе СЗИ. Результаты работ отражаются в организационно-распорядительных документах на ИС и ее СЗИ на этапе эксплуатации.

При реализации процесса e_{32} обсуждаются сведения (в речевой форме) о мерах контроля и разграничения доступа, ограничения прав пользователей, допустимых изменениях условий эксплуатации, состава и конфигурации технических средств и программного обеспечения ИС, о действиях ответственных за реализацию мер защиты информации. Проверка полноты и детальности описания организационных мер защиты осуществляется на основе исследования организационно-распорядительных документов. Раскрытие этих сведений позволит нарушителю на этапе эксплуатации СЗИ ИС скорректировать сценарии реализации УБИ, учитывающие возможности обхода принятых организационных мер защиты.

При реализации процессов e_{33} и e_{34} осуществляется проверка работоспособности и опытная эксплуатация СЗИ ИС, результаты которых оформляются документально. При этом результаты проверки содержат сведения о корректности функционирования этих систем, в том числе с учетом реализованных на предыдущих этапах мер защиты информации, а также о готовности пользователей и администраторов к эксплуатации.

В этапе e_{35} в случае выявления уязвимостей ИС, которые могут привести к возникновению УБИ, не включенных в модель угроз на этапе e_1 (процесс e_{14}), проводится ее уточнение и принимаются дополнительные меры защиты и нформации, направленные на блокирование угроз, связанных с возможностью эксплуатации нарушителем этих уязвимостей. Результаты анализа уязвимостей оформляются в виде документа на электронном и / или бумажном носителе.

Приемочные испытания СЗИ ИС (процесс e_{35}) включают проверку выполнения требований к СЗИ

в соответствии с техническим заданием на их создание. Результаты проверки также оформляются в виде документа на электронном и / или бумажном носителе.

На этапе e_4 с целью проведения аттестационных испытаний ИС и ее СЗИ осуществляется анализ информации, содержащейся в документах, разработанных на этапах $e_1 \div e_3$ в части их соответствия нормативным требованиям (Приказ № 17). На основе экспертно-документального метода при выполнении работ в процессе e_{41} проводится оценка эксплуатационной документации, организационно-распорядительных документов по защите информации и условий функционирования ИС. В процессе e_{42} проводится анализ уязвимостей, связанных с неправильной настройкой программного обеспечения и средств защиты информации, а в процессе e_{43} осуществляются попытки несанкционированного доступа к ИС в обход ее СЗИ. Результаты работ, выполняемых на этапе e_4, включаются в протокол и служат основанием для оформления аттестата соответствия ИС и ее СЗИ требованиям о защите информации. Раскрытие сведений, содержащихся в указанных документах, может быть использовано нарушителем с целью сбоя функционирования оборудования ИС и ее СЗИ, а также реализации УБИ на этапах их эксплуатации и вывода из эксплуатации.

2. Описание процессов обработки информации на различных этапах создания СЗИ объектов информатизации в условиях реализации нарушителем УБИ

В соответствии с существующими подходами к защите информации в ИС и на объекте информатизации для формирования СЗИ и оценки защищенности информации необходимо:

1) определить объект защиты:

– ограждающие конструкции здания и помещения, в пределах которого располагается объект информатизации;

– помещение в составе объекта информатизации, в пределах которого ИС размещается;

– территория здания и прилегающая к нему, информация и / или информационные ресурсы организации);

2) определить УБИ, актуальные для данного объекта защиты;

3) оценить возможности применения доступных мер защиты информации, направленных на блокирование этих угроз.

Кроме того, как показано в [5–8], необходимо учитывать особенности динамики реализации информационных процессов по обработке информации в ИС и на объекте информатизации, а также УБИ.

При проведении работ, выполняемых в интересах создания СЗИ ИС объектов информатизации на различных этапах $e_1 \div e_4$, реализуются информационные процессы (*IPr*) по обработке массивов информации в различных формах ее представления, рассматриваемые в качестве объектов защиты:

$IPr^{(vi)}$ – речевая информация;

$IPr^{(di)}$ – информация в виде документов;

$IPr^{(gi)}$ – графическая информация;

$IPr^{(data)}$ – данные и др.

При реализации *IPr* каждого типа используются соответствующие материальные носители – твердые (бумажные и электронные) и сигнальные (акустические (речевые), электрические, электромагнитные сигналы). Так, содержание приказа о назначении подразделения (e_{11}) может обсуждаться на совещании (мероприятии) путем обмена сообщениями (массива $м_i^{(vi)}, i = \overline{1,I}$) в речевой форме с последующим оформлением результатов мероприятия в виде соответствующего документа (протокола) на бумажном или электронном носителе (массивов $м_j^{(dp)}, j = \overline{1,J}$ и $м_k^{(de)}, k = \overline{1,K}$, соответственно). Для принятия решения о необходимости защиты информации (процесс e_{12}), используемой в интересах деятельности, осуществляется анализ различного рода документов (экономических, финансовых, учредительных и т. п.). Результаты такого анализа могут обсуждаться работниками подразделения на совещаниях в речевой форме ($м_i^{(vi)}$) с последующим оформлением в виде документов ($м_j^{(dp)}$ и $м_k^{(de)}$). Определение класса защищенности ИС (процесс e_{13}) в настоящее время осуществляется на основе экспертных оценок величины ущерба, причиняемого организации (опосредованного ущерба [10]) за счет нарушения основных свойств информации, – прямого ущерба в отношении информации и / или оборудования ИС [10]. При этом осуществляется обсуждение информации ($м^{(vi)}$) в составе подразделения с участием руководителя организации, а результаты оформляются в виде «акта классификации» ($м^{(dp)}$ и $м^{(de)}$). Формирование модели угроз (процесс e_{14}) с использованием программы (https://bdu.fstec.ru/threat-section/shaper-threats) осуществляется с выходом на официальный сайт ФСТЭК России в электронном виде (массива $м_l^{(ei)}, l = \overline{1,L}$) с использованием компьютера, включенного в сеть Интернет. При этом в помещении, в котором установлен компьютер, выполнение шагов по формированию модели угроз и определение модели нарушителя может осуществляться путем дискуссии ($м_i^{(vi)}$) между работниками – участниками данного процесса, а результаты процесса оформляются в виде документа ($м^{(dp)}$ и $м^{(de)}$) – модели угроз, включающей модель нарушителя.

В процессе разработки технического задания на создание ИС и ее СЗИ (процесс e_{15}) формируются предложения о структуре ИС с учетом ее расположения в помещении объекта информатизации, реализуемых структурными элементами функциях, видов обрабатываемой информации, ее материальных носителей и угроз безопасности. Указанные предложения также могут обсуждаться в речевой форме ($м_i^{(vi)}$), а результаты обсуждения оформляются в виде документа – протокола. Документы, создаваемые по результатам реализации процессов $e_{11} \div e_{15}$, оформляются на бумажных и электронных носителях ($м^{(dp)}$ и $м^{(de)}$).

Информационные процессы аналогичных типов ($IPr^{(vi)}$, $IPr^{(di)}$, $IPr^{(gi)}$, $IPr^{(data)}$ и др.) реализуются и при обработке информации, используемой в интересах проведения работ на этапах $e_2 \div e_4$ создания СЗИ ИС в составе объекта информатизации. Как показано в [6], такого рода процессы, во-первых, реализуются во времени, во-вторых, время начала, окончания и продолжительности их реализации случайны, в-третьих, эти процессы, как правило, содержат несколько фрагментов их реализации и пауз между ними, имеющих случайные временны́е характеристики. Кроме того, в составе этих фрагментов сведения, которые могут представлять интерес для нарушителя с точки зрения реализации УБИ как на этапах $e_1 \div e_4$, так и на этапах e_5 и e_6 существования ИС и ее СЗИ, будут присутствовать с некоторой вероятностью p_{vi} или p_{di}. Указанные обстоятельства обусловливают существенные трудности оценки УБИ и защищенности информации на этих этапах на основе экспертных методов существующего нормативного и методического обеспечения (Приказ № 17 и Методика). Для разработки моделей оценки, учитывающих перечисленные условия реализации исследуемых информационных процессов, воспользуемся подходом, приведенным в [2, 5, 6].

На рисунке 2 в качестве примеров приведены временны́е диаграммы реализации $IPr^{(vi)}$ и $IPr^{(di)}$ по обработке информации в речевой и документальной формах, соответственно, при обсуждении результатов выполнения работ (процессы $e_{11} \div e_{15}$) на этапе e_1 «Формирование требований к защите информации»: процесс e_{11} – приказ о назначении структурного подразделения (ответственного) за защиту информации (см. рисунок 2a); процессе e_{12} – решение о необходимости защиты информации и создании СЗИ (см. рисунок 2b)

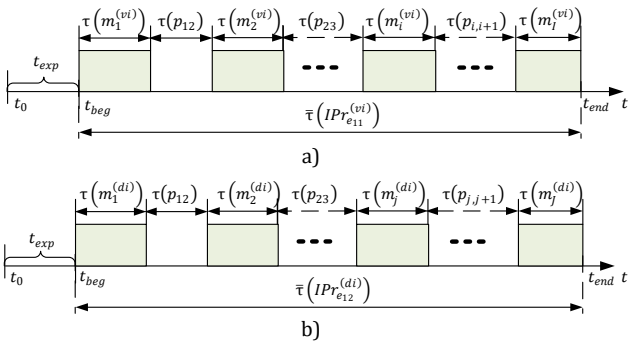

Рис. 2. Временны́е диаграммы реализации информационных процессов по обработке информации в речевой (a) и документальной формах (b)

Fig. 2. Time Diagrams of the Implementation of Information Processes for Processing Information in Speech (a) and Documentary Forms (b)

На рисунке 2 используются следующие обозначения:

t_0 – время начала рабочего дня в организации;

t_{exp} – время ожидания начала совещания (мероприятия);

t_{beg} и t_{end} – времена начала и окончания совещания, соответственно;

$\tau(м_i^{(vi)}), i = \overline{1,I}$ – продолжительность выступления i-го, участника совещания;

$\tau(p_{i,i+1}), i = \overline{1,I-1}$ – продолжительность паузы между выступлениями i-го и $(i+1)$–го участников совещания;

$\bar{\tau}(IPr_{e_{11}}^{(vi)})$ – среднее время реализации процесса e_{11} по обсуждению на совещании работниками организации содержания приказа руководителя о назначении структурного подразделения, ответственного за защиту информации в ИС, создаваемой в интересах обеспечения деятельности организации;

$\tau(p_{j,j+1}), j = \overline{1,J-1}$ – продолжительность паузы между j-м и $(j+1)$–м докладами результатов проделанной работы;

$\tau(м_j^{(di)}), j = \overline{1,J}$ – продолжительность j-го доклада работника о результатах проделанной работы, представленных в документальной форме на бумажном и / или электронном носителе (в том числе с использованием компьютеров, включенных в локальную вычислительную сеть (ЛВС) организации в помещении объекта информатизации).

По результатам совещания оформляется протокол, в котором определяется состав подразделения и его руководитель (для крупных организаций), либо ответственное лицо (для малых организаций), а также определяется перечень сведений, содержание которых носит конфиденциальный характер. Далее будем считать, что в состав такого подразделения включаются несколько работников.

При выполнении работ в процессе e_{12} работниками в соответствии с их обязанностями, определенными руководителем подразделения, осуществляется анализ необходимых документов организации на бумажных или электронных носителях (в случае использования в организации компьютеров, включенных в ЛВС) и составляется отчет по соответствующему разделу. Результаты отчета докладываются на совещании руководителю подразделения. При этом анализ содержания документов работниками может осуществляться параллельно во времени, а его результаты докладываются на совещании последовательно с представлением разработанных документов (см. рисунок 2b).

Временны́е диаграммы, аналогичные представленным на рисунке 2, могут быть использованы для иллюстрации процессов выполнения работ по обработке речевой и документальной информации на других этапах создания СЗИ ИС (процесс e_{14}), в том числе при обсуждении исходных данных вводимых в процессе формирования модели УБИ на различных этапах алгоритма программы ФСТЭК (https://bdu.fstec.ru/threat-section/shaper-threats).

В общем виде описание УБИ включает [7]: «наименование угрозы»; «источник угрозы»; «используемая уязвимость (совокупность уязвимостей)»; «сценарий реализации угрозы»; «объект воздействия»; «несанкционированное действие, выполняемое при реализации угрозы»; «время существования угрозы»; «время, необходимое на реализацию угрозы».

На этапах $e_1 \div e_4$ в качестве деструктивного (несанкционированного) действия в отношении информации, обрабатываемой в интересах создания ИС и ее СЗИ, целесообразно рассматривать нарушение конфиденциальности этой информации, поскольку нарушения ее целостности и / или доступности могут быть выявлены легитимными пользователями, что противоречит одному из основных принципов ведения такого рода действий, – принципа негласности [11]. В связи с этим в качестве объекта воздействия следует рассматривать информационные процессы обработки и речевой ($IPr^{(vi)}$) и документальной информации ($IPr^{(di)}$), соответственно. Нарушение конфиденциальности этой информации является результатом реализации угроз ее утечки, во-первых, по техническим каналам утечки информации (ТКУИ) – с использованием технических средств или без их использования, во-вторых, за счет получения физического или логического (через ЛВС) доступа к компьютерам, используемым для создания необходимых документов. В соответствии с Методикой, источником такого рода угроз могут быть как внутренние, так и внешние нарушители, а также внешние нарушители, выступающие в сговоре с внутренними.

Основным фактором, обусловливающим возможность реализации угрозы утечки речевой информации (массива $м^{(vi)}$), является ее передача при реализации в помещении объекта информатизации информационного процесса $I\mathrm{Pr}^{(vi)}$, а уязвимостью документальной информации (массивов $м^{(de)}$) является ее хранение в памяти компьютеров и передача файлов, содержащих документы, созданные при выполнении работ, по сети ЛВС при реализации информационных процессов $IPr^{(di)}$ или распространение этих документов на бумажных носителях (массивов $м^{(dp)}$) при проведении совещания.

Сценарии реализации рассматриваемых угроз утечки информации определяются применительно к объектам защиты ($IPr^{(vi)}$ и $IPr^{(di)}$) и видам воздействия на них. В соответствии с Методикой, сценарий определяется как последовательность возможных действий, выполняемых нарушителем (внутренним или внешним), имеющим соответствующий уровень возможностей (потенциал), обусловленных наличием в его распоряжении необходимых технических средств для формирования ТКУИ, а также 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. Способом реализации угроз утечки речевой информации (массива $м^{(vi)}$) считается канал ее утечки, в том числе ТКУИ, формируемый внутренним или внешним нарушителями с использованием технических средств приема информативных сигналов или без использования таких средств (формируемый внутренним нарушителем). Возникновение канала утечки информации, обрабатываемой в помещении объекта информатизации организации в интересах создания СЗИ ИС, обусловлено, во-первых, реализацией информационного процесса ($IPr^{(vi)}$ или $IPr^{(di)}$) по обработке информации, представленной в соответствующей форме (речевой или документальной) и подлежащей защите, во-вторых – процесса Pr_u перехвата этой информации нарушителем. В качестве защищаемой информации в данном случае рассматривается речевая ($м^{(vi)}$), содержащая сведения ограниченного распространения, текстовая на бумажном носителе ($м^{(dp)}$), а также файлы на электронных носителях, содержащие такого рода информацию ($м^{(de)}$).

Угрозы утечки документальной информации на бумажных носителях ($м^{(dp)}$) могут быть реализованы за счет применения внутренним нарушителем средств фотофиксации или средств копирова-

ния документов, а в электронном виде файлы, содержащие такого рода информацию ($м^{(de)}$), могут быть перехвачены при их передаче по ЛВС или похищены с использованием вредоносных программ, также внедренных в компьютер внутренним нарушителем.

Если время существования угрозы может быть связано с наличием факторов и / или уязвимостей, которые могут быть использованы для ее реализации, то время, необходимое на ее реализацию, является случайным и в существенной степени зависит от применяемых сценариев и характеризует динамику реализации угрозы.

Указанные обстоятельства обусловливают необходимость при оценке угроз утечки информации, обрабатываемой в интересах создания СЗИ ИС объекта информатизации, и оценке ее защищенности учитывать динамику реализации информационных процессов ($IPr^{(vi)}$ и $IPr^{(di)}$), изменение структурных элементов ИС, используемых в интересах обработки информации, представленной в различном виде (массивов $м^{(vi)}$, $м^{(dp)}$ и $м^{(de)}$), на различных этапах создания ИС и ее СЗИ, а также динамику реализации УБИ на каждом из этих этапов.

Иллюстрация динамики реализации информационных процессов представлена на рисунке 2. Для описания динамики угроз утечки обрабатываемой информации рассмотрим некоторые из множества возможных сценариев их реализации в условиях отсутствия мер защиты.

1. Сценарии реализации угрозы утечки речевой информации внутренним нарушителем:

а) включенным в состав подразделения, выполняющего работы в интересах создания СЗИ, и имеющим доступ на совещания подразделения;

б) выполняющим иные виды деятельности в помещениях организации, смежных с помещениями, в которых проводятся совещания по обсуждению вопросов, связанных с созданием СЗИ, и не допущенным к этим работам.

2. Сценарии реализации угрозы утечки речевой информации внешним нарушителем по ТКУИ [6]:

а) имеющим возможность постоянно находиться в зоне возможного приема информативных сигналов, по параметрам которых может быть раскрыто содержание защищаемой информации, с использованием стационарных и высокотехнологичных технических средств, обеспечивающих выполнение энергетических условий приема;

б) периодически прибывающим в зону возможного перехвата информации с использованием носимых и портативных технических средств, обеспечивающих скрытность их применения.

С учетом вероятностного характера временны́х характеристик сообщений участников совещания, и содержания в этих сообщениях сведений, представляющих интерес для нарушителя, как показано в [7], реализация информационного процесса $IPr^{(vi)}$ или $IPr^{(di)}$ может быть представлена в виде потока событий со средней интенсивностью:

$$\overline{\mu}_{vi} = \frac{1}{\overline{\tau}\left(м^{(vi)}\right) + \overline{\tau}(p)}, \; \overline{\mu}_{di} = \frac{1}{\overline{\tau}\left(м^{(di)}\right) + \overline{\tau}(p)}.$$

В этих условиях в качестве показателя возможностей утечки информации в течение каждого из процессов $e_{11} \div e_{15}$ выполнения работ на этапе e_1, по аналогии с [6, 7], будем использовать вероятность $P_{i1}^0(t), i = \overline{1,5}$ перехвата хотя бы одного сообщения, содержащего сведения, представляющие интерес для внутреннего нарушителя, при выполнении работ, проводимых в течение одного из процессов ($e_{11} \div e_{15}$) за заданное время в условиях отсутствия мер защиты.

При экспоненциальном приближении вероятность перехвата сообщения рассчитывается по формуле [6]:

$$\begin{aligned} P_{i1}^0(t) &= 1 - \exp(-\overline{\mu_{vi}} \cdot p_{vi} \cdot t), \\ P_{i1}^0(t) &= 1 - \exp(-\overline{\mu_{di}} \cdot p_{di} \cdot t). \end{aligned} \quad (1)$$

В [7] обоснована правомерность такого приближения при вероятностях $p_{vi} < 0{,}4$, $p_{di} < 0{,}4$, а с увеличением этих вероятностей вероятность перехвата соответствующих сообщений $P_{i1}^0(t) \to 1$.

Если необходимо оценить возможность перехвата не менее *N* сообщений при выполнении работ проводимых в течение одного из процессов $e_{11} \div e_{15}$, например, на этапе e_1, то выражение (1) преобразуется к следующему виду [6]:

$$P_{1,\geq N}^0(t) = \sum_{n=N}^{M} \frac{(\overline{\mu_{v1}} \cdot p_{v1} \cdot t)^n}{n!} \cdot \exp(-\overline{\mu_{v1}} \cdot p_{v1} \cdot t), \quad (2)$$

где M – количество участников совещания; $\overline{\mu_{v1}}$ – средняя интенсивность передачи речевых или документированных сообщений при проведении совещания по результатам выполнения работ в течение одного из процессов $e_{11} \div e_{15}$ на этапе e_1 создания СЗИ ИС; p_{v1} – вероятность того, что в этих сообщениях содержится информация, представляющая интерес для нарушителя.

Для всех $e_{11} \div e_{15}$ процессов вероятность перехвата хотя бы одного сообщения, представляющего интерес для нарушителя, вычисляется по формуле:

$$P_{i,1}^0(t) = 1 - \prod_{i=1}^{5} \left[1 - P_{i,1}^0(t)\right], \quad (3)$$

для не менее, чем *N* сообщений:

$$P_{5,\geq N}^0(t) = 1 - \prod_{i=1}^{5} \left[1 - P_{5,\geq N}^0(t)\right]. \quad (4)$$

Временны́е диаграммы, характеризующие динамику сценария 1б реализации угроз утечки речевой информации в условиях отсутствия мер защиты, приведены на рисунке 3. Внутренний нарушитель имеет возможность лишь периодически осуществлять перехват информации путем «прослушивания» переговоров из смежного помещения, или при нахождении под каким-либо предлогом у неплотно прикрытой двери, а также в случае отсутствия каких-либо ограничений на нахождение в помещении, в котором осуществляются переговоры, как организационной меры защиты информации.

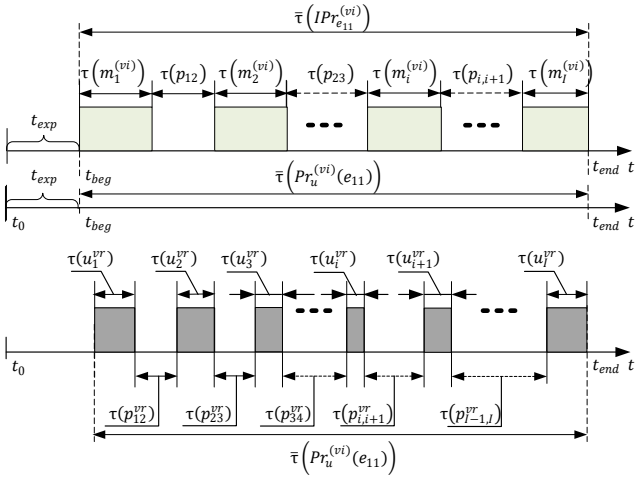

Рис. 3. Временны́е диаграммы сценария реализации угрозы утечки речевой информации при выполнении работ в процессе e_{11} на этапе e_1, внутренним нарушителем (без мер защиты)

Fig. 3. Time Diagrams of the Scenario for the Implementation of the Threat of Leakage of Speech Information When Performing Work in the e_{11} Process at the e_1 Stage, by an Internal Intruder (without Protective Measures)

На рисунке 3 используются следующие обозначения:

$\tau(u_i^{vr}), i = \overline{1,I}$ – время реализации i-й попытки перехвата речевого сообщения во время проведения совещания;

$\tau\left(p_{i,i+1}^{vr}\right), i = \overline{1,I}$ – продолжительность паузы между i-й и $(i+1)$ попытками перехвата речевого сообщения во время проведения совещания;

$\bar{\tau}\left(Pr_u^{(vi)}(e_{11})\right)$ – средняя продолжительность реализации угрозы утечки речевой информации во время проведения совещания по результатам выполнения работ в процессе e_{11} на этапа e_1 формирования СЗИ.

При этом, по аналогии с [6, 7], процесс реализации перехвата информации представляется в виде потока попыток перехвата с некоторой их средней продолжительностью $\bar{\tau}(u^{vr})$ и средней интенсивностью во время проведения совещания по результатам выполненных работ на этапе e_1 создания СЗИ:

$$\overline{\mu}^{vr} = \frac{1}{\bar{\tau}(u^{vr}) + \bar{\tau}(p^{vr})}, \quad \overline{\mu}^{vd} = \frac{1}{\bar{\tau}(u^{vd}) + \bar{\tau}(p^{vd})},$$

где $\bar{\tau}(u^{vr}), \bar{\tau}(u^{vd})$ – средние продолжительности попыток перехвата речевого сообщения и документа, соответственно; $\bar{\tau}(p^{vr}), \bar{\tau}(p^{vd})$ – средние продолжительности пауз между попытками перехвата речевых сообщений и документов, соответственно.

Поток событий, соответствующих прибытию нарушителя к месту возможного перехвата речевых сообщений, описывается средней интенсивностью $\overline{\mu}^{vr}$ и средней продолжительностью $\bar{\tau}(u^{vr})$, а поток событий, соответствующих передаче речевых сообщений во время проведения совещания по результатам выполнения работ в течение соответствующего процесса на этапе e_1 создания СЗИ, содержащих конфиденциальную информацию, – средней интенсивностью $\overline{\mu_{vi}}$ и средней продолжительностью $\bar{\tau}(\text{м}^{(vi)})$. Тогда возможность перехвата одного сообщения при отсутствии мер защиты будет определяться вероятностью совпадения этих потоков [6, 7]:

$$P_1^0(t) = 1 - \exp\left[-\overline{\mu_{vi}} \cdot \overline{\mu}^{vr}\left(\bar{\tau}(\text{м}^{(vi)}) + \bar{\tau}(u^{vr})\right) p_{vi} t\right]. \quad (5)$$

Возможность перехвата не менее N сообщений определим по выражению (6).

$$P_{1,\geq N}^0(t) = \sum_{n=N}^{M} \frac{\left(\overline{\mu_{v1,j}} \cdot \overline{\mu}^{vr}\left(\bar{\tau}(\text{м}^{(vi)}) + \bar{\tau}(u^{vr})\right) \cdot p_{v1,j} t\right)^n}{n!} \exp\left(-\overline{\mu_{v1,j}} \cdot \overline{\mu}^{vr}\left(\bar{\tau}(\text{м}^{(vi)}) + \bar{\tau}(u^{vr})\right) p_{v1,j} t\right). \quad (6)$$

Для оценки возможности утечки речевой (документированной) информации при проведении работ в течение всех процессов на этапе e_1 будем использовать (3 и 4).

Аналогичный подход может быть использован для оценки вероятности реализации угрозы утечки речевой информации внешним нарушителем. В случае реализации сценария 2а будем применять выражения, аналогичные (2–4), а для сценария 2б – формулы (5 и 6). При этом возможность постоянного нахождения нарушителя в зоне возможного

перехвата информации (при отсутствии адекватных мер защиты) позволяет ему с большей вероятностью раскрыть содержание сообщений, обрабатываемых на этапе e_1 в интересах создания СЗИ ИС объекта информатизации.

3. Описание процессов защиты информации на различных этапах создания СЗИ ИС

В соответствии с существующим нормативным и методическим обеспечением, защита информации от угроз ее утечки должна осуществляться на всех этапах создания ИС и ее СЗИ путем блокирования этих угроз с учетом особенностей описаний сценариев динамики их реализации в различных условиях.

В настоящее время в составе каждого из базовых наборов мер защиты, в соответствии с Приказом № 17, предусмотрены меры защиты технических средств:

– организация контролируемой зоны вокруг объекта информатизации;

– контроль и управление физическим доступом к структурным элементам ИС и СЗИ, к средствам обеспечения их функционирования, в помещения и сооружения, в которых эти элементы и средства установлены;

– размещение устройств отображения информации, исключающее ее несанкционированный просмотр нарушителем.

Очевидно, что меры такого характера могут быть применены для защиты информации, содержащей приведенные выше сведения, и в процессе создания СЗИ объектов информатизации. Следует отметить, что в настоящее время указанные меры могут быть реализованы на основе информационно-сигнализационных систем, представляющих собой совокупность функционально объединенных датчиков различной физической природы, средств вычислительной техники и технических средств извлечения, приема и передачи информации [2], известных (в соответствии с Методикой) как системы охранного мониторинга. Такие системы используются и в государственных, и в негосударственных организациях, в первую очередь, в интересах реализации мер физической защиты информации путем применения организационных мероприятий и совокупности технических средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты, предусматривающих установление режимных, временны́х, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты [1]. Следует отметить, что указанные мероприятия осуществляются с использованием превентивно установленных средств и не позволяет учитывать динамику параллельно реализуемых процессов обработки информации на различных этапах создания СЗИ, ее перехвата нарушителем как внутренним, так и внешним, и блокирования угроз перехвата информации в этих условиях.

Для защиты информации от утечки в рассматриваемых условиях целесообразно применять организационные и технические меры, адаптированные к выполнению нарушителем действий по реализации процессов $Pr_u^{(vi)}$ и $Pr_u^{(vi)}$. К организационным мерам, по аналогии с [6], следует отнести создание мобильных групп в составе 2–3 человек для физического контроля территории, прилегающей к контролируемой зоне (зданию, помещению) объекта информатизации, в составе которого создается СЗИ и ИС, действующих под управлением администратора информационно-сигнальной системы, контролирующего обстановку на этой территории с применением систем видеонаблюдения (стационарных или мобильных). Мобильные группы проводят осмотр этой территории для обнаружения места, с которого нарушитель (внутренний или внешний) может применять средства перехвата информации. К техническим мерам относятся применение мобильных устройств, которыми оснащаются эти группы, используемых для выявления возможных действий нарушителя, периодически прибывающего в зону возможного перехвата информации в пределах контролируемой зоны и на территории, прилегающей к ней.

Эффект защиты заключается в возможности своевременного обнаружения действий по перехвату информации (или подготовке к перехвату) и оперативного привлечения к пресечению этих действий работников из мобильных групп при их появлении в пределах видимости нарушителя. При этом как организационные, так и технические меры являются опережающими, то есть они оказываются эффективными, если нарушитель в результате их применения не успевает перехватить конфиденциальную информацию. Указанные меры часто применяются на практике, однако оценка угроз утечки информации в условиях применения указанных мер и динамики реализации угроз не проводилась.

Рассмотрим применение некоторых мер защиты при подготовке и реализации IPr^{vi} на этапах создания СЗИ объекта информатизации. Поскольку способом реализации угрозы утечки информации является сценарий реализации канала ее утечки, будем рассматривать применение этих мер применительно к блокированию действий нарушителя по реализации этого сценария. Меры защиты могут быть превентивными, проводимыми до реализации IPr^{vi}, или осуществляемыми в ходе его реализации.

В первом случае, когда соответствующий канал утечки не ликвидируется с вероятностью $1 - p_{det}^{vi}$, где p_{det}^{vi} – вероятность обнаружения канала утечки информации, возможность ее перехвата определяется вероятностью того, что канал не ликвидирован, и временны́ми характеристиками передачи сообщений, содержащих сведения, представляющие интерес для нарушителя в процессе выполнения работ в интересах создания СЗИ.

С учетом (1) вероятность перехвата одного сообщения при обсуждении результатов работ, выполняемых, например, в процессе e_{11} на этапе e_1 создания СЗИ в ходе реализации IPr^{vi} в течение времени t, рассчитывается по формуле [6]:

$$P_{i1}^{ZI}(t) = 1 - \exp\left[-\overline{\mu_{vi}} \cdot p_{vi} \cdot \left(1 - p_{det}^{vi}\right) \cdot t\right]. \qquad (7)$$

Вероятность перехвата не менее N сообщений, содержащих конфиденциальную информацию при обсуждении результатов работ, выполняемых в процессе e_{11} на этапе e_1 создания СЗИ в ходе реализации IPr^{vi} в течение времени t, рассчитывается по формуле (8).

$$P_{i,\geq N}^{(\text{ЗИ})}(t) = \sum_{n=N}^{M} \frac{\left[\overline{\mu_{v1}} \cdot p_{v1} \cdot \left(1 - p_{det}^{vi}\right) \cdot t\right]^n}{n!} \exp\left[-\overline{\mu_{v1}} \cdot p_{v1} \cdot \left(1 - p_{det}^{vi}\right) \cdot t\right]. \qquad (8)$$

Для всех $e_{11} \div e_{15}$ процессов вероятность перехвата хотя бы одного сообщения, представляющего интерес для нарушителя, вычисляется как:

$$P_{i,1}^{ZI}(t) = 1 - \prod_{i=1}^{5}\left[1 - P_{i,1}^{ZI}(t)\right], \qquad (9)$$

для не менее, чем N сообщений:

$$P_{5,\geq N}^{ZI}(t) = 1 - \prod_{i=1}^{5}\left[1 - P_{5,\geq N}^{ZI}(t)\right]. \qquad (10)$$

Если меры защиты осуществляются в ходе реализации процессов IPr^{vi} и $Pr_u^{(vi)}$, существует множество логических условий, связанных с необходимостью выполнения различного рода действий в интересах подготовки реализации этих процессов. Как показано в [6], учет этих условий возможен с использованием моделей на основе аппарата составных сетей Петри – Маркова. Разработка таких моделей является предметом дальнейших исследований авторов.

Заключение

Защита информации, используемой в интересах создания ИС, должна осуществляться на всех этапах ее создания. Это связано с тем, что раскрытие содержания как самой информация, так и ее фрагментов, может использоваться нарушителем для реализации УБИ, обрабатываемой в ИС на этапе ее эксплуатации, что может привести к нанесению ущерба деятельности организации, в интересах которой ИС создается.

Сложности реализации мер защиты в отношении информации, обрабатываемой в интересах создания ИС и ее СЗИ, и обоснования организационно-технического обеспечения их реализации на различных этапах их создания, обусловлены отсутствием в настоящее время: описаний взаимосвязанных и параллельно реализуемых процессов обработки этой информации, как объектов защиты; сценариев процессов реализации угроз нарушения ее конфиденциальности на различных этапах, а также процессов защиты информации, учитывающих их реализацию во времени, случайный характер временны́х признаков различных фрагментов и выполняемых действий, а также наличие различного рода логических условий их реализации. Парирование этих сложностей может быть достигнуто путем представления исследуемых процессов в виде потоков событий на основе теории потоков. В целях учета логических условий динамики исследуемых процессов, определяющих возможность их реализации, возникает необходимость разработки моделей для вычисления их случайных временны́х характеристик на основе аппарата составных сетей Петри – Маркова.

При описании процессов обработки информации, используемой в интересах создания ИС и ее СЗИ на объекте информатизации, как объектов защиты на различных этапах их создания, возникает ряд вопросов, связанных с определением видов информации, ее материальных носителей, номенклатуры оборудования, используемого для обработки, а также последовательности и содержания работ, выполняемых на каждом из этапов. Изменения объектов защиты обусловливают изменения условий возникновения и реализации угроз нарушения конфиденциальности этой информации и возможностей выполнения нарушителем различных сценариев их реализации.

Оценка УБИ на различных этапах создания ИС и ее СЗИ, а также оценка защищенности информации от реализации этих угроз, невозможны без соответствующего организационно-технического и методического обеспечения. Сегодня такое обеспечение

отсутствует, а его создание связано с необходимостью решения вопросов разработки математических моделей оценки угроз в условиях динамики их реализации с учетом фактора времени и различных логических условий, включающих описательные (вербальные) модели, учитывающие последовательность и содержание действий выполняемых при реализации различного рода процессов обработки информации в различных условиях обстановки, совокупность уязвимостей этих процессов, как объектов защиты, показателей для проведения такой оценки в условиях отсутствия и применения мер защиты, а также аналитических соотношений для их вычисления, обоснования организационно-технического обеспечения в составе организационных и технических мер защиты.

Для оценки УБИ предложено использовать систему количественных показателей. Для расчета таких показателей с учетом фактора времени при отсутствии мер защиты или в условиях применения превентивно установленных мер целесообразно использовать аналитические выражения на основе теории потоков. Приведены примеры применения этого аппарата для количественной оценки угроз утечки речевой и документированной информации для сценариев их реализации внутренним и внешним нарушителем в различных условиях обстановки при отсутствии мер защиты и с учетом применения превентивно установленных мер. Для учета логических условий, определяющих процесс реализации угроз, целесообразно использовать аппарат составных сетей Петри – Маркова.

Список источников

1. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. М.: Стандартинформ, 2009.

2. Avsentiev O.S., Valde A.G., Konkin Yu.V. Ensuring the Protection of Information in the Process of Creating an Information System of an Informatization Object // Chemistry and Technology of Fuels and Oils. 2021. № 3. P. 36.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2007.

4. Авсентьев О.С., Вальде А.Г. К вопросу о формировании системы защиты информации от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений объектов информатизации // Вестник Воронежского института МВД России. 2021. № 2. С. 22–33. EDN:VNLGMX

5. Язов Ю.К., Авсентьев О.С., Авсентьев А.О., Рубцова И.О. Метод оценивания эффективности защиты электронного документооборота с применением аппарата сетей Петри – Маркова // Труды СПИИРАН. 2019. Т. 18. № 6. С. 1269–1300. DOI:10.15622/sp.2019.18.6.1269-1300. EDN:FBTRZZ

6. Avsentiev O.S., Avsentiev A.O., Krugov A.G., Yazov Yu.K. Simulation of processes for protecting voice information objects against leakage through the spurious electromagnetic radiation channels using the Petri – Markov nets // Journal of Computational and Engineering Mathematics. 2021. Vol. 8. Iss. 2. PP. 3–24. DOI:10.14529/jcem210201. EDN:VOKXXO

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

8. Язов Ю.К., Анищенко А.В., Суховерхов А.С. Основы теории составных сетей Петри-Маркова и их применения для моделирования процессов реализации угроз безопасности информации в информационных системах. Монография. СПб.: Сциентиа, 2024. 196 с. DOI:10.32415/scientia_978-5-6052111-2-9. EDN:CGTNTU

9. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М.: Стандартинформ, 2014.

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

11. Меньшаков Ю.К. Теоретические основы технических разведок: учебное пособие. Под ред. Ю.Н. Лаврухина. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 536 с.

References

1. GOST 34.601-90. *Information technology. Set of standards for automated systems. Automated systems. Stages of development*. Moscow: Standartinform Publ.; 2009. (in Russ.)

2. Avsentiev O.S., Valde A.G., Konkin Yu.V. Ensuring the Protection of Information in the Process of Creating an Information System of an Informatization Object. *Chemistry and Technology of Fuels and Oils*. 2021;3:36.

3. GOST R 50922-2006. *Protection of information. Basic terms and definitions.* Moscow: Standartinform Publ.; 2007. (in Russ.)

4. Avsentev O.S., Valde A.G. To the question of formation of information protection system from leakage through technical channels occurring due to side electromagnetic radiation on informatization objects. *The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2021;2:22–33. (in Russ.) EDN:VNLGMX

5. Yazov Yu.K., Avsentev O.S., Avsentev A.O., Rubcova I.O. Method for Assessing Effectiveness of Protection of Electronic Document Management Using the Petri and Markov Nets Apparatus. *SPIIRAS Proceedings*. 2019;18(6):1269–1300. (in Russ.) DOI:10.15622/sp.2019.18.6.1269-1300. EDN:FBTRZZ

6. Avsentiev O.S., Avsentiev A.O., Krugov A.G., Yazov Yu.K. Simulation of processes for protecting voice information objects against leakage through the spurious electromagnetic radiation channels using the Petri - Markov nets. *Journal of Computational and Engineering Mathematics*. 2021;8(2):3–24. DOI:10.14529/jcem210201. EDN:VOKXXO

7. Yazov Yu.K., Anishchenko A.V. *Petri-Markov Networks and Their Application for Modelling Processes of Information Security Threats Implementation in Information Systems*. Voronezh: Kvarta Publ.; 2020. 173 p. (in Russ.)

8. Yazov YU.K., Anishchenko A.V., Suhoverhov A.S. *Fundamentals of the Theory of Composite Petri-Markov Networks and Their Application for Modelling the Processes of Implementation of Information Security Threats in Information Systems*. St. Petersburg: Scientia Publ.; 2024. 196 p. (in Russ.) DOI:10.32415/scientia_978-5-6052111-2-9. EDN:CGTNTU

9. GOST R 51583-2014. *Information protection. Sequence of protected operational system formation. General provisions*. Moscow: Standartinform Publ.; 2014. (in Russ.)

10. Yazov Yu.K., Solov'ev S.V. *Methodology for Assessing the Effectiveness of Information Protection in Information Systems against Unauthorised Access*. St. Petersburg: Naukoemkie tekhnologii Publ.; 2023. 258 p. (in Russ.) EDN:WVCHKW

11. Menshakov Yu.K. *Theoretical Foundations of Technical Reconnaissance*. Ed. Yu.N. Lavruhina. Moscow: Bauman MSTU Publ.; 2008. 536 p. (in Russ.)

Статья поступила в редакцию 11.09.2024; одобрена после рецензирования 21.10.2024; принята к публикации 23.10.2024.
The article was submitted 11.09.2024; approved after reviewing 21.10.2024; accepted for publication 23.10.2024.

Информация об авторах:

АВСЕНТЬЕВ Олег Сергеевич | доктор технических наук, профессор, профессор кафедры информационной безопасности Воронежского института МВД России

БУТОВ Владислав Вячеславович | кандидат технических наук, начальник кафедры информационной безопасности Воронежского института МВД России

ВАЛЬДЕ Андрей Геннадьевич | заместитель начальника – начальник отдела центра информационных технологий, связи и защиты информации Управления МВД России по Амурской области

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.