УДК: 007.51, 004.032.24, 608.3 DOI: 10.53816/23061456_2021_9–10_52

АВТОМАТИЗИРОВАННЫЙ КОНТРОЛЬ И УПРАВЛЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

AUTOMATED CONTROL AND MANAGEMENT OF TECHNICAL INFORMATION SECURITY OF INFORMATIZATION OBJECTS

Д.Н. Алексеев, д-р техн. наук О.А. Финько

D.N. Alekseev, D.Sc. O.A. Finko

Краснодарское высшее военное училище им. С.М. Штеменко

Предложен способ автоматизированного контроля и управления технической защитой информации объектов информатизации от утечки по каналам побочных электромагнитных излучений и наводок. Обеспечивается необходимый уровень защищенности информации, обрабатываемой как на локализованных, так и на распределенных объектах информатизации в режиме реального времени. Идея основана на выполнении мониторинга возникновения возможных каналов утечки информации через побочные электромагнитные излучения и наводки, применении резервных средств технической защиты информации в случае их проявления. Приведен вариант реализации способа в виде автоматизированной системы.
Ключевые слова: объект информатизации, мониторинг электромагнитных излучений, техническая защита информации, автоматизированная система.

A method of automated control and management of technical protection of information from leakage through the channels of compromising emanations is proposed. The method allows providing the necessary level of information security on localized and distributed objects of informatization in real time. The idea of the method is based on monitoring the occurrence of possible channels of information leakage through spurious electromagnetic emanations and the use of backup means of technical protection of information in the event of their manifestation. A variant of the implementation of the method in the form of an automated system is given.
Keywords: object of informatization, monitoring of electromagnetic emanations, technical protection of information, automated system.

Введение

Эксплуатация объектов информатизации (ОИ) неразрывно связана с рисками утечки информации по техническим каналам, среди которых одним из наиболее опасных является неконтролируемое распространение побочных электромагнитных излучений и наводок (ПЭМИН), возникающих при работе средств вычислительной техники (СВТ). Кроме того, на защищенность ОИ может оказывать воздействие неэффективная работа средств технической защиты информации (ТЗИ) [1].

Функционирование СВТ и средств ТЗИ сопровождается влиянием различных факто-

ров объективного и субъективного характера. К основным объективным факторам относятся внезапно возникающие дефекты, сбои, отказы технических средств (ТС) и систем ОИ, приводящие к изменению параметров электромагнитных излучений и способствующих наилучшему перехвату техническими средствами разведки, а также влияющие на эффективность работы средств ТЗИ. Основными субъективными факторами могут быть нарушения функционирования ТС в результате ошибок при эксплуатации ТС и систем защиты информации, связанные со случайным и (или) преднамеренным воздействием пользователей или обслуживающего персонала.

На различных стадиях эксплуатации рассмотренные ОИ факторы оказывают различное влияние на вероятность образования технических каналов утечки информации (ТКУИ). Очевидно, чем длительнее срок эксплуатации ОИ между интервалами контроля, тем эта вероятность повышается. Возникает проблемная ситуация, когда проведение инструментального контроля с нормативно определенной периодичностью не способно обеспечить своевременное обнаружение угроз утечки информации по техническим каналам и, как следствие, принятие эффективных мер по их устранению [2].

Описание предлагаемого способа и вариант его технического исполнения

Входные данные — множества:

$\mathbf{M} = \{m_1, m_2, \ldots, m_i\}$ — множество СВТ, где i — количество подвергаемых контролю основных технических средств и систем с наиболее опасными режимами работы;

$\mathbf{G} = \{g_1, g_2, \ldots, g_j\}$ — множество средств ТЗИ, где j — количество установленных для защиты информации генераторов шума;

$\mathbf{D} = \{d_1, d_2, \ldots, d_k\}$ — множество пространственныхнаправлений размещения СВТ и генераторов шума, где k — количество локализованных мест размещения отдельных частей ОИ;

$\mathbf{F} = \{\Delta f_1, \Delta f_2, \ldots, \Delta f_4\}$ — множество частотных полос контроля информативных сигналов СВТ и генераторов шума;

$\mathbf{R} = \{r_1, r_2, \ldots, r_z\}$ — множество контрольных приемников, где z — количество анализаторов сигналов, применяемых для мониторинга информативных сигналов ПЭМИ;

$\mathbf{A} = \{a_1, a_2, \ldots, a_z\}$ — множество приемных антенн, применяемых для мониторинга;

$\mathbf{G}^{\text{рез}} = \{g_1^{\text{рез}}, g_2^{\text{рез}}, \ldots, g_n^{\text{рез}}\}$ — множество резервных средств ТЗИ, где n — количество резервных генераторов шума, применяемых по результатам контроля ТЗИ, $n \le j$;

$\mathbf{V} = \{v_1, v_2, \ldots, v_r\}$ — множество элементов распределенной антенной системы подсистемы резервной активной ТЗИ, где r — количество излучающих антенн, применяемых по результатам контроля ТЗИ, $r \le k$.

Введем предикаты:

$$E_i^{(m)}(t_{\text{контр}}), E_j^{(g)}(t_{\text{контр}}) = \begin{cases} 1, & \text{если} \quad \sigma_{\text{контр}} > \sigma_{\text{норм}}; \\ 0, & \text{если} \quad \sigma_{\text{контр}} \le \sigma_{\text{норм}}, \end{cases}$$

где $E_i^{(m)}(t_{\text{контр}})$ — параметр, характеризующий уровень излучения информативных сигналов ПЭМИ m_i-го СВТ множества $\mathbf{M}$; $E_j^{(g)}(t_{\text{контр}})$ — параметр, характеризующий уровень маскирующего излучения g_j-го средства ТЗИ множества $\mathbf{G}$; $\sigma_{\text{контр}}$ — показатель защищенности по результатам мониторинга; $\sigma_{\text{норм}}$ — нормированное значение показателя защищенности; $t_{\text{контр}}$ — периодичность проведения контроля АСКУ ТЗИ.

Параметр $E_i^{(m)}(t_{\text{контр}})$ характеризуется частотной и пространственной составляющими:

$$E_i^{(m,f)}(t) \in \left\{E_1^{(m,f)}(t), E_2^{(m,f)}(t), \ldots, E_i^{(m,f)}(t), \ldots, E_q^{(m,f)}(t)\right\};$$
$$E_i^{(m,d)}(t) \in \left\{E_1^{(m,d)}(t), E_2^{(m,d)}(t), \ldots, E_i^{(m,d)}(t), \ldots, E_u^{(m,d)}(t)\right\}.$$

Матрица контролируемых параметров СВТ:

$$\left(\mathbf{E_i^{(m,f,d)}}\right)_{\mathbf{q \times u}},$$

где q — порядковый номер строки, а u — порядковый номер столбца матрицы.

Матрица контролируемых параметров средств ТЗИ:

$$\left(\mathbf{E_j^{(g,f,d)}}\right)_{\mathbf{q \times u}}.$$

Учитывая, что изменение состояния защищенности ОИ зависит от вероятности изменения

контролируемых параметров, и, заменяя их на вероятности проявления, при которых показатель защищенности превышает нормированное значение (опасное состояние), получаем матрицы вероятностей возникновения ТКУИ, способствующих ее перехвату:

$$\left(\mathbf{P}_{\mathbf{i}}^{(\mathbf{m,f,d})}\right)_{\mathbf{q\times u}} \quad \text{и} \quad \left(\mathbf{P}_{\mathbf{j}}^{(\mathbf{g,f,d})}\right)_{\mathbf{q\times u}}.$$

Отсюда следует, что характеристика общего состояния защищенности ОИ — вероятность опасного состояния:

$$P_{\text{ткуи}}(t)\{\vee E_{q,u}^{(m,g,f,d)}(t_{\text{контр}})=1\}.$$

Задача поддержания требуемого уровня защиты информации может быть решена за счет применения способа и автоматизированной системы, которые позволяют контролировать состояние работоспособности генераторов шума (ГШ), применяемых для защиты информации на ОИ, параметры ПЭМИН, возникающих при работе СВТ, и управлять показателем защищенности непосредственно в процессе функционирования:

$$\langle \mathbf{M},\mathbf{G},\mathbf{D},\mathbf{F},\mathbf{R},\mathbf{A},\mathbf{G}^{\text{рез}},\mathbf{V}\rangle \to \{P_{\text{ткуи}}(t)\} \mid \forall \{\mathbf{M}\{m_1,m_2,\ldots,m_i\};\quad \mathbf{G}\{g_1,g_2,\ldots,g_j\};$$
$$\mathbf{D}\{d_1,d_2,\ldots,d_k\};\quad \mathbf{F}\{\Delta f_1,\Delta f_2,\ldots,\Delta f_4\}\}: P_{\text{обн}}(t_{\text{контр}}) \to \max \wedge (P_{\text{ткуи}}(t_{\text{пер}}) \le P_{\text{пор}}(t_{\text{пер}})),$$

где $P_{\text{обн}}(t_{\text{контр}})$ — вероятность выявления отклонения контролируемых параметров от их допустимых значений; $P_{\text{ткуи}}(t_{\text{пер}})$ — вероятность наступления опасного состояния ОИ, при котором возможен перехват информативных сигналов ПЭМИ; $P_{\text{пор}}(t_{\text{пер}})$ — пороговое значение вероятности наступления опасного состояния; $t_{\text{пер}}$ — период эксплуатации ОИ до очередного нормативно определенного проведения контроля эффективности защиты информации.

Это достигается путем автоматизации анализа результатов контроля и мониторинга и, выборочно или во всем диапазоне частот, маскирования возникающих опасных информативных сигналов и компенсирования ухудшения характеристик зашумления (изменение полосы генерируемых шумов, уменьшение спектральной плотности мощности или спектральной плотности напряженности поля шумового сигнала) штатно установленных ГШ за счет применения резервных программно-управляемых ГШ и распределенной антенной системы, излучающие элементы которой размещаются в направлении вероятного ведения разведки потенциальным противником. Обобщенная структурная схема ОИ с установленными ГШ представлена на рис. 1.

Обобщенная структурная схема ОИ и автоматизированной системы контроля и управления технической защитой информации ОИ от утечки по каналам побочных электромагнитных излучений и наводок (АСКУ ТЗИ) представлена на рис. 2.

АСКУ ТЗИ работает под управлением оператора, состоит из подсистем, включающих функциональные блоки и технические средства:

– оператор АСКУ ТЗИ;

– подсистема контроля ТЗИ;

– подсистема управления ТЗИ;

– подсистема резервной активной ТЗИ.

Оператор АСКУ ТЗИ обеспечивает включение/выключение системы и контроль ее функционирования.

На рис. 3 представлена структурная схема подсистемы контроля ТЗИ, состоящей из:

– анализаторов сигналов (АС) с приемными антеннами (АнС), расположенными в ближней зоне ТС ОИ;

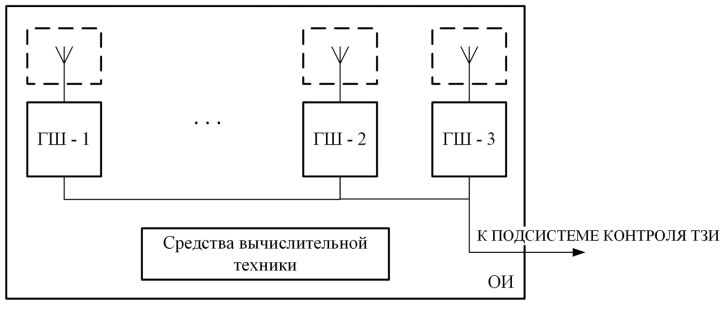

Рис. 1. Структурная схема объекта информатизации с установленными генераторами шума

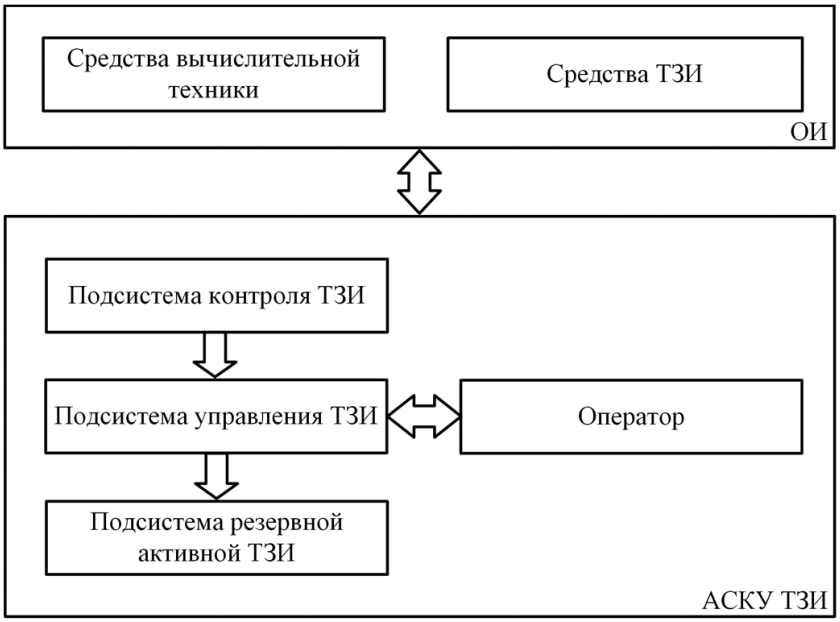

Рис. 2. Обобщенная структурная схема объекта информатизации и автоматизированной системы контроля и управления технической защитой информации объектов информатизации от утечки по каналам побочных электромагнитных излучений и наводок

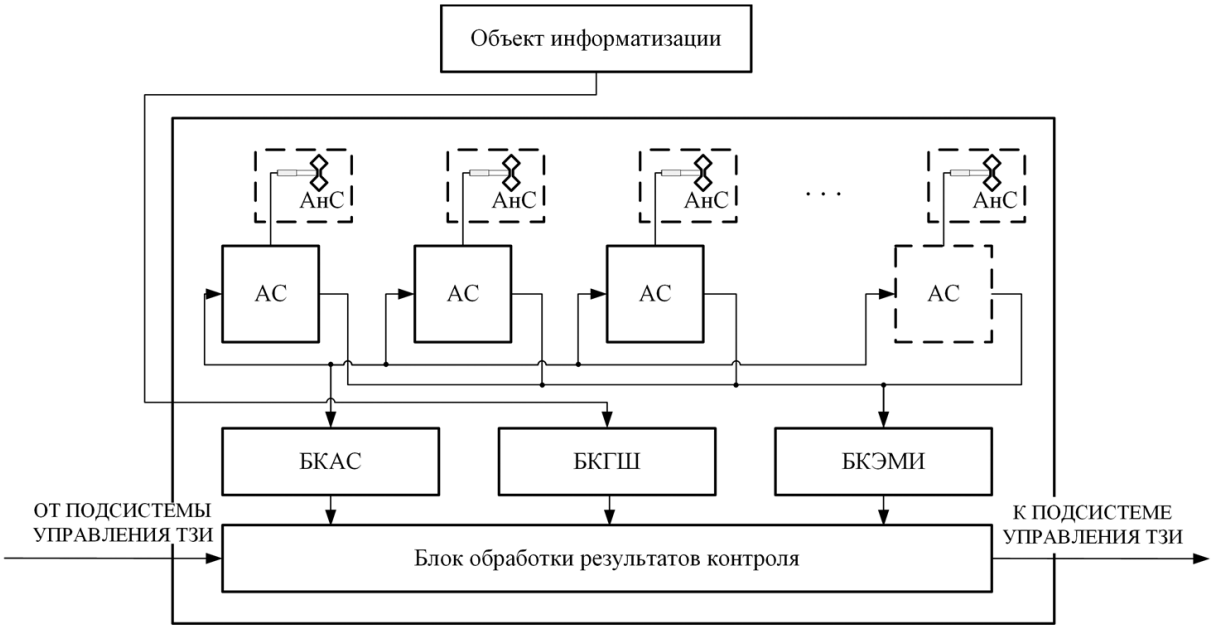

Рис. 3. Структурная схема подсистемы контроля технической защиты информации

– блока контроля анализаторов сигналов (БКАС), который обеспечивает контроль их функционирования и управление режимами работы;

– блока контроля генераторов шума (БКГШ), который обеспечивает контроль их включенного состояния и работоспособности;

– блока контроля электромагнитных излучений (БКЭМИ), который обеспечивает контроль ПЭМИ ТС ОИ и широкополосных излучений генераторов шума;

– блока обработки результатов контроля (БОРК), который обеспечивает обобщение результатов контроля работоспособности и мони-

торинга электромагнитных излучений и передачу управляющих информационных сигналов к подсистеме управления ТЗИ.

На рис. 4 представлена структурная схема подсистемы управления ТЗИ (ПУ ТЗИ), состоящей из:

– блока интерфейсов (БИ), обеспечивающих сопряжение с остальными подсистемами;

– вычислительного управляющего устройства (ВУУ), обеспечивающего необходимые операции расчета и формирование сигналов управления;

– блока хранения данных (БХД), в котором хранится информация о настройках оборудования, результатах контроля и мониторинга, дополнительные данные об ОИ, необходимые при расчетах защищенности обрабатываемой информации и контроле функционирования ГШ («частотная маска» контролируемого диапазона частот, коэффициент реального затухания электромагнитного поля и др.);

– блока отображения (БО), который обеспечивает отображение функционирования АСКУ ТЗИ и подачу необходимых сигналов оператору;

– блока ввода/вывода (БВВ), который обеспечивает запуск и управление функциями АСКУ ТЗИ и обновление дополнительной информации в БХД.

Подсистема управления ТЗИ может быть выполнена в виде автоматизированного рабочего места, представляющего собой ПЭВМ с установленным специальным программным обеспечением (СПО), обеспечивающим управление функциями программно-аппаратных средств АСКУ ТЗИ, формирование интерфейса оператора, защиту от воздействия вредоносного программного обеспечения и несанкционированного доступа.

На рис. 5 представлена структурная схема подсистемы резервной активной ТЗИ (ПРА ТЗИ), состоящей из:

– блока резервных программно-управляемых генераторов шума (БРПУГШ), позволяющих генерировать маскирующие электромагнитные излучения в заданных ПУ ТЗИ полосах частот с необходимой мощностью;

– коммутирующего устройства (КУ), позволяющего распределять сигналы БРПУГШ;

– излучающих элементов (ИЭ) распределенной резервной антенной системы (РРАНС), позволяющей излучать маскирующие электромагнитные излучения на заданных ПУ ТЗИ участках ОИ.

На этапе подготовки АСКУ ТЗИ к работе в БХД заносятся данные о составе и настройках ТС ОИ, результаты предварительных измерений ПЭМИ ТС ОИ, ГШ и параметры затухания электромагнитного поля. Производится установка СПО для управления БКАС, БКГШ и БКЭМИ, а также расчета показателя защищенности обрабатываемой информации для управления ПРА ТЗИ. На всех ПЭВМ из состава ОИ устанавливается СПО для запуска тестовых режимов поиска и измерения параметров ПЭМИН.

В ходе функционирования АСКУ ТЗИ в случае несовпадения результатов мониторинга ПЭМИ ТС с ранее внесенными и хранящимися в БХД параметрами (увеличение уровня или появление новых информативных сигналов ПЭМИ) с помощью СПО выполняется расчет

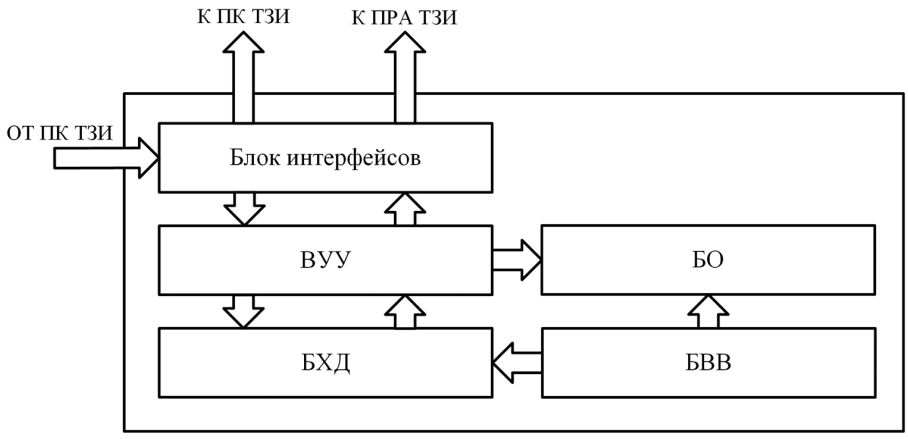

Рис. 4. Структурная схема подсистемы управления технической защитой информации

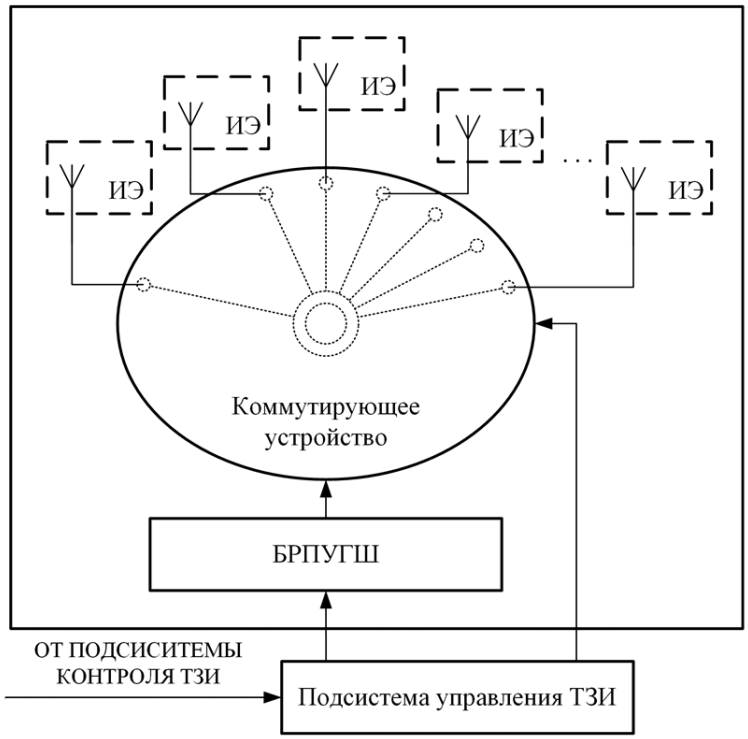

Рис. 5. Структурная схема подсистемы резервной активной технической защиты информации

защищенности обрабатываемой информации с учетом результатов контроля работоспособного состояния и мониторинга электромагнитных излучений штатных ГШ. При невыполнении установленных норм защиты информации с помощью СПО выполняется расчет необходимой мощности маскирующих излучений в выявленных полосах частот, подаются управляющие сигналы ПРА ТЗИ для активации БРПУГШ и выбора требуемых излучающих элементов из РРАНС. Далее, выполняется контроль состояния работоспособности и функционирования штатных ГШ с заданной АСКУ ТЗИ периодичностью. При возникновении сбоев и отказов в их работе происходит автоматический расчет требуемой мощности маскирующих излучений в необходимых полосах частот и активация ПРА ТЗИ.

Результаты численных исследований

Технический результат используемого способа и системы подтверждается построением аналитической и математической моделей образования технических каналов утечки информации за счет ПЭМИН с различной периодичностью проведения контроля защищенности.

Рассмотрев взаимосвязь наступления различных событий, таких как появление постепенных или внезапных отказов и сбоев ТС ОИ, вызванных естественным старением электронной компонентной базы, преждевременным износом ТС ОИ, вызванным режимами работы или неправильной эксплуатацией, можно сделать вывод, что ОИ в любой момент времени будет находиться в одном из состояний:

S1 — отсутствие ТКУИ, способствующих ее перехвату;

S2 — наступление деградационных отказов, влияющих на образование ТКУИ;

S3 — наступление внезапных отказов, влияющих на образование ТКУИ;

S4 — образование ТКУИ, способствующих ее перехвату;

S5 — обнаружение и устранение ТКУИ при проведении регламентированного периодического контроля.

Граф возможных состояний ОИ, на котором проводится регламентированный периодический контроль эффективности защиты информации, а также возможные переходы из одного состояния в другое, представлены на рис. 6.

Матричная форма системы дифференциальных уравнений [3] для данного графа с принятыми в качестве допущения интенсивностями переходов:

$$\frac{\mathbf{d}}{\mathbf{dt}}\begin{bmatrix}\mathbf{P_1}\\ \mathbf{P_2}\\ \mathbf{P_3}\\ \mathbf{P_4}\\ \mathbf{P_5}\end{bmatrix}=\begin{pmatrix}-(\lambda_{12}+\lambda_{13}) & 0 & 0 & 0 & \lambda_{51}\\ \lambda_{12} & -(\lambda_{23}+\lambda_{24}) & 0 & 0 & 0\\ \lambda_{13} & \lambda_{23} & -\lambda_{34} & 0 & 0\\ 0 & \lambda_{24} & \lambda_{34} & -\lambda_{45} & \lambda_{54}\\ 0 & 0 & 0 & \lambda_{45} & -(\lambda_{51}+\lambda_{54})\end{pmatrix}\cdot\begin{pmatrix}P_1\\ P_2\\ P_3\\ P_4\\ P_5\end{pmatrix},$$

где $\lambda_{12}=200$, $\lambda_{13}=700$, $\lambda_{23}=10$, $\lambda_{24}=100$, $\lambda_{34}=1700$, $\lambda_{45}=500$, $\lambda_{51}=500$, $\lambda_{54}=200$.

При применении на ОИ АСКУ ТЗИ появляется еще одно состояние системы S6, которое оказывает влияние на возможное состояние ОИ — это обнаружение и устранение ТКУИ между интервалами проведения регламентированного периодического контроля. На рис. 7 показаны возможные состояния ОИ и переходы из одного состояния в другое.

Матричная форма системы дифференциальных уравнений для данного графа:

$$\frac{\mathbf{d}}{\mathbf{dt}}\begin{bmatrix}\mathbf{P_1}\\ \mathbf{P_2}\\ \mathbf{P_3}\\ \mathbf{P_4}\\ \mathbf{P_5}\\ \mathbf{P_6}\end{bmatrix}=\begin{pmatrix}-(\lambda_{12}+\lambda_{13}) & 0 & 0 & 0 & \lambda_{51} & \lambda_{61}\\ \lambda_{12} & -(\lambda_{23}+\lambda_{24}) & 0 & 0 & 0 & 0\\ \lambda_{13} & \lambda_{23} & -\lambda_{34} & 0 & 0 & 0\\ 0 & \lambda_{24} & \lambda_{34} & -(\lambda_{45}+\lambda_{46}) & \lambda_{54} & \lambda_{64}\\ 0 & 0 & 0 & \lambda_{45} & -(\lambda_{51}+\lambda_{54}) & 0\\ 0 & 0 & 0 & \lambda_{46} & 0 & -(\lambda_{61}+\lambda_{64})\end{pmatrix}\cdot\begin{pmatrix}P_1\\ P_2\\ P_3\\ P_4\\ P_5\\ P_6\end{pmatrix},$$

где $\lambda_{12}=200$, $\lambda_{13}=700$, $\lambda_{23}=10$, $\lambda_{24}=100$, $\lambda_{34}=1700$, $\lambda_{45}=500$, $\lambda_{46}=700$, $\lambda_{51}=500$, $\lambda_{54}=200$, $\lambda_{61}=700$, $\lambda_{64}=50$.

Зависимости вероятностей образования ТКУИ в процессе эксплуатации ОИ при регламентированном периодическом контроле защищенности и с применением АСКУ ТЗИ соответственно представлены на рис. 8 и 9.

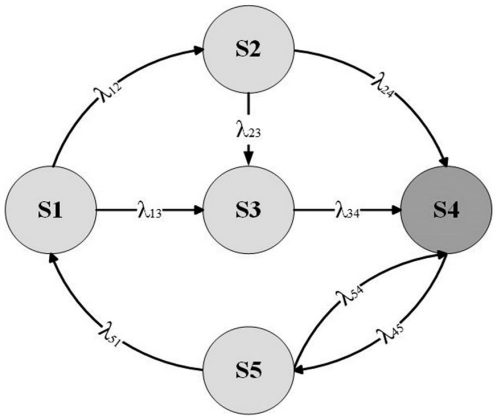

Рис. 6. Граф состояний объекта информатизации, на котором проводится периодический контроль эффективности защиты информации

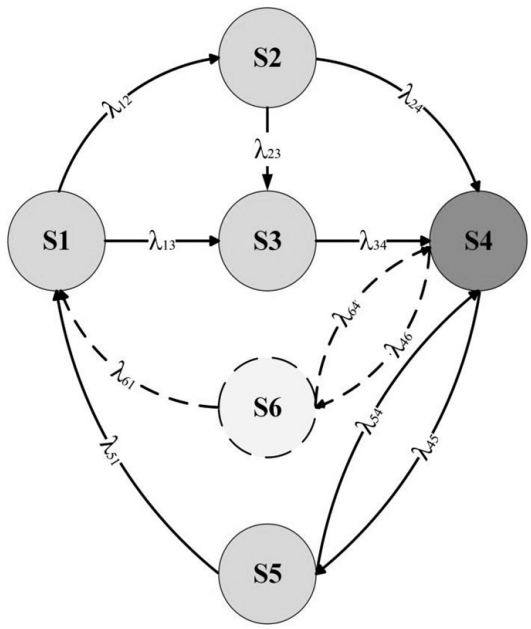

Рис. 7. Граф состояний объекта информатизации, на котором применяется автоматизированная система контроля и управления технической защитой информации

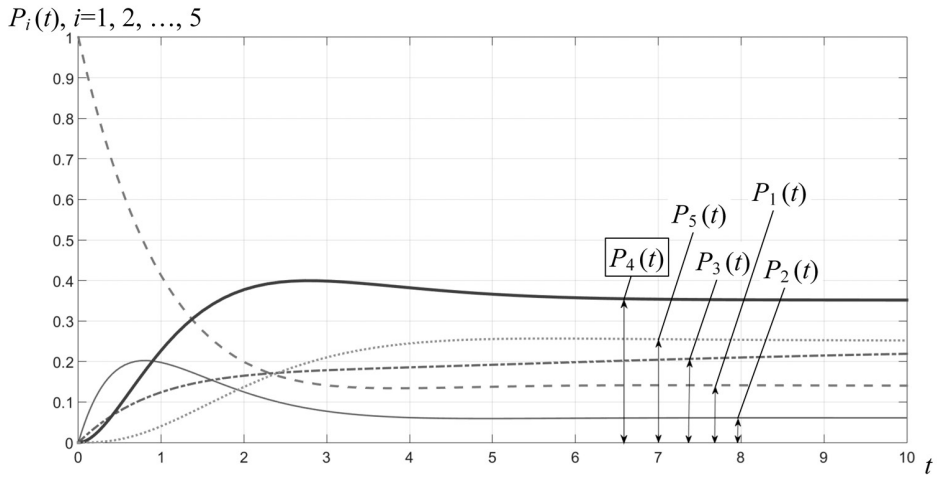

Рис. 8. Зависимости вероятностей $P_i(t),\ i=1,2,...,5,$ *при периодическом контроле эффективности защиты информации*

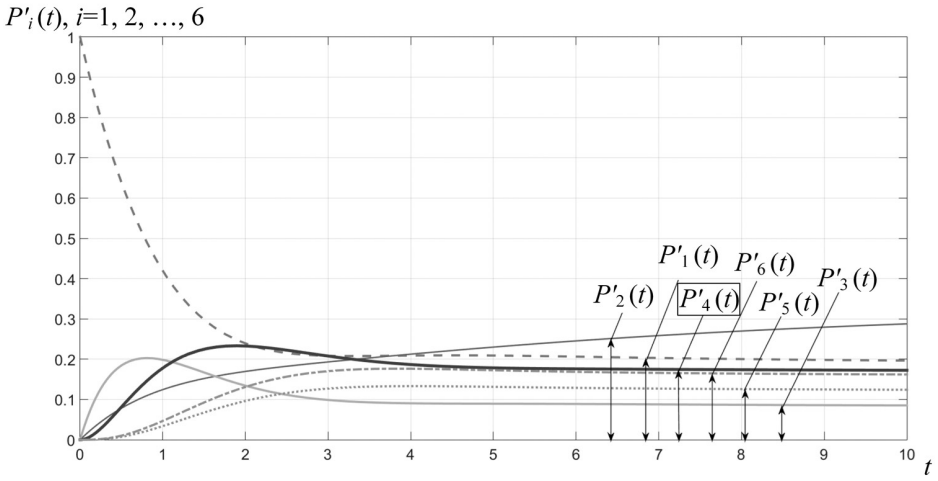

Рис. 9. Зависимости вероятностей $P_i^{'}(t),\ i=1,2,...,6,$ *с применением АСКУ ТЗИ*

Из рис. 8 и 9 следует, что применение АСКУ ТЗИ снижает вероятность нахождения объекта в состоянии возникновения ТКУИ, способствующих перехвату информации. Полученные в результате расчета значения вероятностей $P_4(t)=0,35$ и $P_4^{'}(t)=0,18$ позволяют оценить эффективность предлагаемого решения, что в процентном отношении составляет приблизительно 48,6 %.

Выводы

Предложенные решения позволяют обеспечить:

– выявление сбоев и отказов в работе технических средств ОИ в реальном масштабе времени или с заданным шагом периодичности, влияющих на возможности возникновения ТКУИ через ПЭМИН;

– автоматизированное управление защищенностью от утечки по каналам ПЭМИН в режиме реального времени за счет применения резервной подсистемы технической защиты информации;

– непрерывность безопасного функционирования СВТ из состава ОИ при выполнении критически важных задач.

Литература

1. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов: в 3 т. Т. 1. Технические каналы утечки информации /

под ред. Ю.Н. Лаврухина. — М.: Аналитика. 2008. 436 с.

2. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. Учебник для вузов / Под ред. А.П. Зайцева и А.А. Шелупанова. 7-е изд., испр. — М.: Горячая линия–Телеком. 2016. 442 с.

3. Нетес В.А. Основы теории надежности. Учебное пособие для вузов. — М.: Горячая линия–Телеком. 2019. 102 с.

4. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. — СПб: НИУ ИТМО. 2011. 112 с.

5. Хорев А.А. Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Ч. 2 / Специальная техника. 2011. № 4. С. 51–62.

6. Советов Б.Я., Яковлев С.А. Моделирование систем: учеб. для вузов: 3-е изд., перераб. и доп. — М.: ГУП Издательство Высшая школа. 2001. 343 с.

7. Ким Д.П. Теория автоматического управления. Т. 1 Линейные системы. — М.: ФИЗМАТЛИТ. 2003. 288 с.

8. Мезенцев К.Н. Моделирование систем. В 2 ч. Ч. 1 Основы системотехники и исследования систем: курс лекций / под ред. д-ра техн. наук, проф. А.Б. Николаева. — М.: МАДИ. 2017. 84 с.

9. Зорин А.В., Зорин В.А., Пройдакова Е.В., Федоткин М.А. Введение в общие цепи Маркова: учебно-методическое пособие. — Нижний Новгород: Нижегородский госуниверситет. 2013. 51 с.

10. Кремер Н.Ш. Теория вероятностей и математическая статистика. — М.: ЮНИТИ. 2004. 573 с.

References

1. Khorev A.A. Technical protection of information. Vol. 1. Technical channel of information leakage. — Moscow: Analitika. 2008. 436 p.

2. Zaytsev A.P., Mescheryakov R.V., Shelupanov A.A. Technical means and methods of information protection. — Moscow: Goryachaya liniya–Telekom. 2016. 442 p.

3. Netes V.A. Fundamentals of reliability theory. — Moscow: Goryachaya liniya–Telekom. 2019. 102 p.

4. Gatchin Y.A. and Klimova E.V. Introduction to comprehensive information protection. — Saint Petersburg: NIU ITMO. 2011. 112 p.

5. Khorev A.A. Evaluation of the possibility for intercepting side electromagnetic radiation of the computer video system part 2 / Spetsial'naya tekhnika. 2011. № 4. P. 51–62.

6. Sovetov B.Ya., Yakovlev S.A. Modeling of systems: Ucheb. dlya vuzov: 3 izd., pererab. i dop. — Moscow: GUP Izdatel'stvo Vysshaya shkola. 2001. 343 p.

7. Kim D.P. Theory of automatic control. Vol. 1. Linear systems. — Moscow: FIZMATLIT. 2003. 288 p.

8. Mezentsev K.N. Modeling of systems. Part 1. Fundamentals of system engineering and system research. — Moscow: MADI. 2017. 84 p.

9. Zorin A.V., Zorin V.A., Proidakova E.V., Fedotkin M.A. Introduction to general Markov chains. — Nizhniy Novgorod: Nizhegorodskiy gosuniversitet. 2013. 51 p.

10. Kremer N.Sh. Probability theory and mathematical statistics. — Moscow: YUNITI. 2004. 573 p.