**DOI: 10.25728/iccss.2022.46.38.062**

**Сидоренко И.А., Силюнцев С.В., Кураков В.А.**

# Оценка временных показателей решения задач радиомониторинга перспективной пространственно-распределенной системой

**Аннотация:** Приведены результаты экспресс-оценки требуемых показателей заблаговременного решения задач радиомониторинга пространственно-распределенной системой радио- и радиотехнического контроля в условиях конфликтного взаимодействия с системой технической разведки.

**Ключевые слова:** информационный конфликт, средства радио- и радиотехнического контроля, технические средства разведки

Стремительное развитие и повсеместное применение современных радиоэлектронных систем, применяемых для решения широкого спектра задач разведки, связи, навигации, радиоэлектронной борьбы и других не менее важных задач, значительно увеличивает нагрузку на радиочастотный спектр, усложняя задачу ведения радио- и радиотехнического контроля (РРТК). Учитывая количество, мощности и диапазон рабочих частот современных радиоэлектронных систем, можно сделать вывод, что усовершенствование радиоприемных устройств проходит не так оперативно, а вследствие чего становится невозможным одновременный охват всех объектов РРТК. Кроме того, сейчас наблюдается интенсивный рост возможностей радио- и радиотехнической разведки, как основного источника получения разведывательной информации. Поэтому в настоящее время перед специалистами комплексного технического контроля (КТК) и разработчиками перспективной техники КТК стоит задача оптимально подобрать время контроля типовых объектов РРТК (диапазона частот), в целях упреждающего выполнения задач информационного конфликта технических средств разведки (ТСР) и средств радио- и радиотехнического контроля (РРТК) мер противодействия (ПД) ТСР. Выполнение этой задачи сводится к

необходимости заблаговременному выявлению нарушений мер ПД ТСР на объектах контроля, что является ключевым условием достижения требуемого уровня защиты информации.

Оценка текущего уровня готовности средств РРТК к заблаговременному решению информационных задач, в условиях постоянно нарастающего конфликта средств РРТК и ТСР, является актуальной задачей, важнейшей целю которой, является заблаговременное выявление нарушений мер по ПД ТСР, для оперативного принятия мер к их устранению (ослаблению) и снижению эффективности применения ТСР.

Для успешного решения указанной задачи проведено структурное представление процесса рассматриваемого конфликта, представленное на рисунке 1. Такое представление существенно облегчает понимание конфликта между сложными системами. Схема отражает основные этапы ведения РРТК, выявление каналов утечки информации и принятия мер к их закрытию (ослаблению). При анализе состояний объекта контроля, вероятностей переходных процессов из состояния в состояние, а также динамику информационного конфликта, каждая из вероятностей перехода объекта из одного состояния в другое будет зависеть только от времени и текущего состояния. Таким образом, система интегро-дифференциальных уравнений, описывающих данный конфликт, имеет следующий вид

$$\begin{gathered}
\tilde{P}_1(t) = P_{1\text{н}} \cdot \delta(t) + P_{81} \int_0^t \varphi_{81}(t-\tau) \cdot \tilde{P}_8(\tau) d\tau, \\
\dots \\
\tilde{P}_8(t) = P_{8\text{н}} \cdot \delta(t) + P_{68} \int_0^t \varphi_{68}(t-\tau) \cdot \tilde{P}_6(\tau) d\tau, \\
\tilde{P}_9(t) = P_{9\text{н}} \cdot \delta(t) + P_{79} \int_0^t \varphi_{79}(t-\tau) \cdot \tilde{P}_7(\tau) d\tau \\
+ P_{69} \int_0^t \varphi_{69}(t-\tau) \cdot \tilde{P}_6(\tau) d\tau,
\end{gathered} \tag{1}$$

где $\tilde{P}_i(t)$ – вероятность того, что объект контроля в течение бесконечно малого интервала времени $(\mathrm{t}, \mathrm{t}+\mathrm{dt})$ перейдет в состояние $C_i$; $P_{ij}$ и $\varphi_{ij}(t)$ – соответственно вероятность и функция

плотности вероятности перехода объекта из состояния $C_i$ в состояние $C_j$; $P_{i\text{н}}$ – вероятность нахождения объекта в состоянии $C_i$ в момент времени $\mathrm{t} = 0$; $\sum_{i=1}^{4} P_{i\text{н}} = 1$; $\delta(t)$ – дельта-функция Дирака.

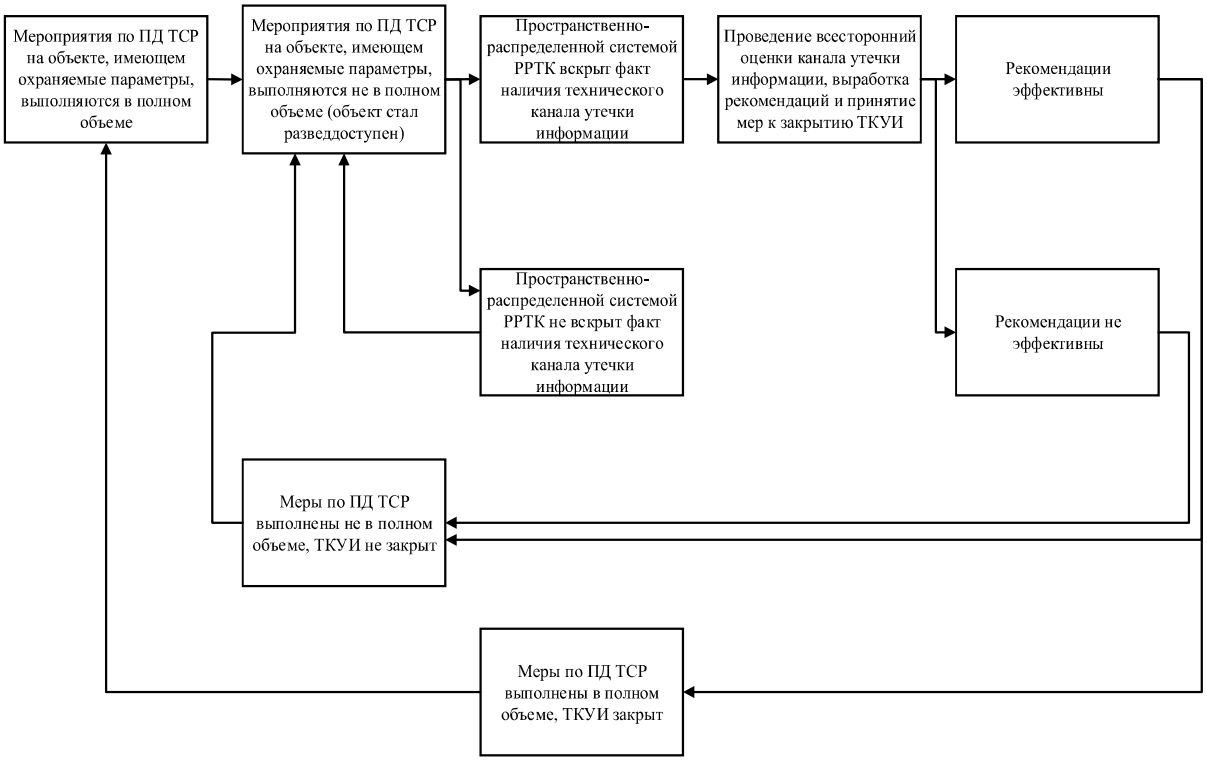


Рисунок 1 – Структурное представление процесса информационного конфликта средств РРТК и сигнальных технических разведок

Для перехода упрощения формулы вероятности обозначим через $H_j^+(t)$ и $H_j^-(t)$ среднее число переходов рассматриваемого процесса в интервале $(0, \mathrm{t})$, после каждого из которых процесс попадает в состояние $C_i$ и покидает состояние $C_j$. Учитывая то, что дифференциалы функций восстановления $dH_j^+(t)$ и $\mathrm{d}H_j^-(t)$ интерпретируются как вероятности того, что в интервале времени $(\mathrm{t}, \mathrm{t} + \mathrm{dt})$ произойдут соответствующие переходы, то для данного случая указанные дифференциалы функции восстановления примут следующий вид

$$dH_i^+(t) = P_i, \text{ где } i=1\ldots9,$$

$$dH_1^-(t) = P_{12}\int_0^t \varphi_{12}(t-\tau)\cdot\tilde{P}_1(\tau)d\tau,$$

$$dH_2^-(t) = P_{23}\int_0^t \varphi_{23}(t-\tau)\cdot\tilde{P}_2(\tau)d\tau$$

$$+P_{24}\int_0^t \varphi_{24}(t-\tau)\cdot\tilde{P}_2(\tau)d\tau, \qquad (2)$$

$$\ldots$$

$$dH_9^-(t) = P_{91}\int_0^t \varphi_{91}(t-\tau)\cdot\tilde{P}_9(\tau)d\tau.$$

Таким образом, полученные функции восстановления позволяют построить математическую модель рассматриваемого информационного конфликта, представленную на рисунке 2.

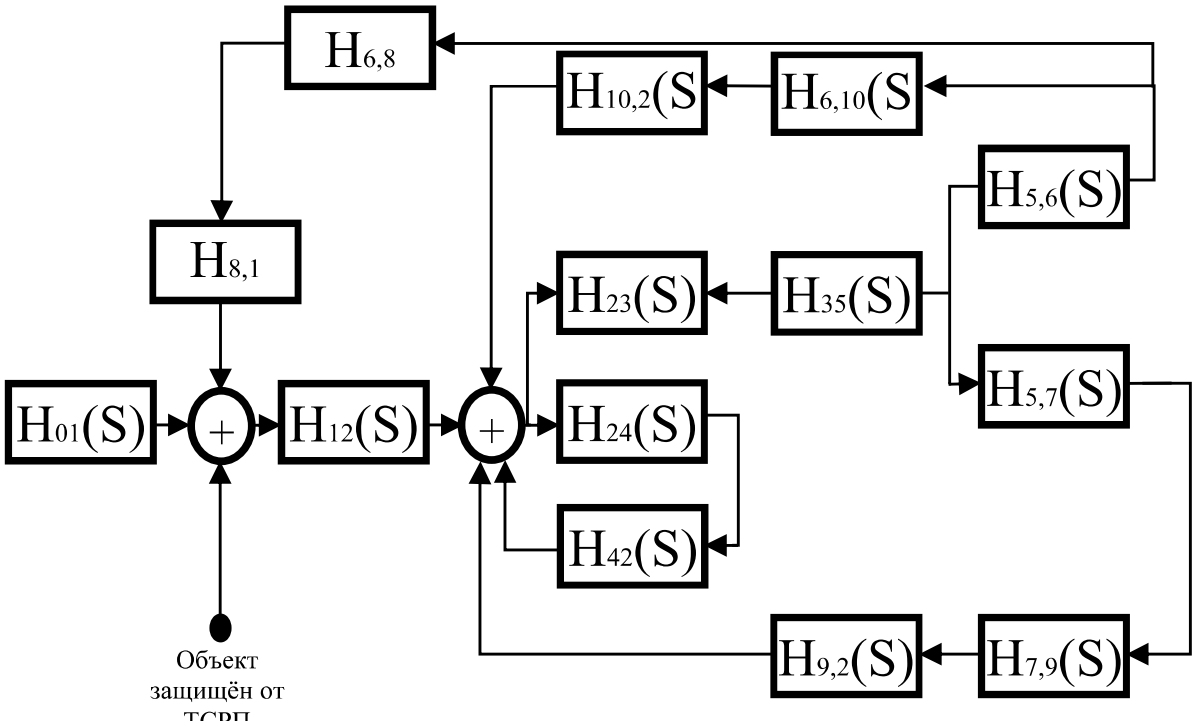


Рисунок 2 – Математическая модель информационного конфликта средств РРТК и ТСР

Вероятности нахождения объекта контроля в системе можно представить следующим образом

$$P_1(t) = \int_0^t \{dH_1^+(u) - dH_1^-(u)\}du =$$
$$= P_{1н} + P_{81} \cdot \int_0^t \int_0^u \varphi_{81}(u-\tau) \cdot \tilde{P}_8(\tau)dtdu - P_{12}$$
$$\cdot \int_0^t \int_0^u \varphi_{12}(u-\tau) \cdot \tilde{P}_1(\tau)dtdu,$$
$$\dots$$
$$P_9(t) = \int_0^t \{dH_9^+(u) - dH_9^-(u)\}du =$$
$$= P_{9н} + P_{69} \cdot \int_0^t \int_0^u \varphi_{69}(u-\tau) \cdot \tilde{P}_6(\tau)dtdu + P_{79}$$
$$\cdot \int_0^t \int_0^u \varphi_{79}(u-\tau) \cdot \tilde{P}_7(\tau)dtdu - P_{92}$$
$$\cdot \int_0^t \int_0^u \varphi_{92}(u-\tau) \cdot \tilde{P}_9(\tau)dtdu,$$

(3)

Применив преобразование Лапласа, данную систему уравнений можно преобразовать к виду

$$L\{P_1(t)\} = P_1(s) = \frac{1}{s} \cdot \begin{bmatrix} P_{1н} + P_{81} \cdot \varphi_{81}(s) \cdot \tilde{P}_8(s) \\ -P_{81} \cdot \varphi_{81}(s) \cdot \tilde{P}_8(s) \end{bmatrix},$$
$$\dots$$
$$L\{P_9(t)\} = P_9(s) = \frac{1}{s} \cdot \begin{bmatrix} P_{9н} - P_{92} \cdot \varphi_{92}(s) \cdot \tilde{P}_9(s) \\ +P_{69} \cdot \varphi_{69}(s) \cdot \tilde{P}_6(s) \\ +P_{79} \cdot \varphi_{79}(s) \cdot \tilde{P}_7(s) \end{bmatrix},$$

(4)

где $\tilde{P}_i(s)$ и $\varphi_{ij}(s)$ – соответственно, преобразования Лапласа от $\tilde{P}_i(t)$ и $\varphi_{ij}(t)$.

Для определения оптимального времени упреждающего выполнения информационных задач перспективной пространственно-распределенной системой радио- и радиотехнического контроля обозначим случайные моменты времени, в которых объект контроля разведдоступен и неразведдоступен, то есть $\tau_{C_1}$ – мероприятия по ПД ТСР

выполняются в полном объеме, $\tau_{C_2}$ – мероприятия по ПД ТСР выполняются не в полном объеме. Функция плотности вероятности разницы сравниваемых моментов времени есть не что иное, как свертка плотностей вероятностей случайных величин $\tau_{C_1}$ и $\tau_{C_2}$

$$W_{C_1}(\tau_{C_1} - \tau_{C_2}) = \int_0^{\infty} \varphi_{C_1}(t) \cdot \varphi_{C_2}(t - \tau_{C_1} + \tau_{C_2})dt. \quad (5)$$

Отсюда вероятность нахождения объекта в состоянии $C_1$ не менее t единиц времени будет определяться интегралом от выражения (5)

$$P_{C_1}(t > t_c) = \int_{t_c}^{\infty} W_{C_1}(\tau_{C_1} - \tau_{C_2})d\tau. \quad (6)$$

Аналогично (6) может быть найдена вероятность нахождения объекта РРТК в состоянии $C_2$, а полученные значения могут быть применены для расчета времени упреждающего выполнения информационных задач.

Таким образом, основываясь на полученных результатах, не трудно определить конкретные значения требуемого времени выполнения задач по ведению РРТК, которые должны находиться в пределах от единиц миллисекунд до единиц секунд. Полученные результаты могут быть успешно применены как при проектировании перспективных комплексов РРТК, так и при оценке, распределении и постановки задач имеющимся силам и средствам комплексного технического контроля. Учитывая предельно малый диапазон времени, отводимые на решение информационных задач, значительно усложняют задачу мгновенного выявления существующих каналов утечки информации, с целью упреждающего принятия мер к его закрытию, до его вскрытия СТР, и свидетельствует о необходимости повышения оперативности решения задач КТК, автоматизации процесса ведения РРТК, анализа выявленных каналов утечки информации и принятии мер к их закрытию.

Литература:

1. *Козирацкий Ю.Л.* Модели информационного конфликта средств поиска и обнаружения. Монография. – М.: Радиотехника, 2013. – 232 с.

2. *Леньшин А.В., Кравцов Е.В., Славнов К.В.* Методика оценки эффективности защиты информации на объектах комплексного технического контроля // Радиотехника. – 2021. – №1. – С. 20-27.

3. *Кравцов Е.В.* Методический подход к комплексной оперативной оценке возможностей выявления сведений об объектах защиты // Телекоммуникации. – 2020. – № 9. – С. 33-41.

**DOI: 10.25728/iccss.2022.22.51.063**

**Еронин Д. А., Мелихов А.А.**

## Разработка автоматизированного средства, предназначенного для выявления потенциально опасных конфигураций ИС малого предприятия

**Аннотация:** В работе рассматривается проблематика использования средств обнаружения уязвимостей в конфигурации ИС малого предприятия и предложено решение позволяющие автоматически проводить регулярный аудит и выявлять уязвимости.

**Ключевые слова:** обнаружение уязвимостей, сканер безопасности, аудит безопасности, управление уязвимостями

### Введение

Поддержание надёжного функционирования бизнес-процессов и обеспечение конфиденциальности данных сегодня актуально для любого типа предприятия - как большого, так и малого. Однако возможностей для построения системы обеспечения безопасности у малого предприятия значительно меньше. Это вызвано как бюджетными ограничениями, так и отсутствием финансовой возможности найма отдельных специалистов, занимающихся непосредственно обеспечением информационной безопасности. В итоге, задача обеспечения информационной безопасности предприятия ложится на системного администратора, для которого