Методика комплексной оценки состояния информационной безопасности региональной группировки войск

Полковник в запасе Ю.Е. ДОНСКОВ,
доктор военных наук

Полковник в запасе Е.Т. ДЮНДИКОВ,
кандидат технических наук

Подполковник в запасе А.А. КАЧКИН,
кандидат технических наук

НЕПРЕРЫВНОЕ совершенствование характеристик и возможностей средств информационного противоборства в военной сфере диктует необходимость постоянной модернизации и адаптации структуры, состава методического обеспечения оценки состояния информационной безопасности группировок войск[1,2].

Под информационной безопасностью понимается состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз[3].

Концепция национальной безопасности Российской Федерации[4,5] укрепление информационной безопасности ставит в ряд важнейших долгосрочных задач.

К объектам обеспечения информационной безопасности (ИБ) в сфере обороны относятся[6,7]:

информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

---

[1] Шерстюк В.П. Актуальные проблемы обеспечения информационной безопасности Российской Федерации // Военная Мысль. 2003. №6. С. 28 — 32.

[2] Родионов С.Н. Политика и информационная безопасность государства в условиях военных конфликтов // Военная мысль. 2005. №6. С. 16 — 21.

[3] Закон РФ от 5 марта 1992 г. №2446-1 «О безопасности».

[4] Концепция национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 10 января 2000 г. №24 // СЗ РФ. 2000. №2. Ст. 170.

[5] Концепция национальной безопасности Российской Федерации // Вестник военной информации. 2002. №2.

[6] Микрюков В.Ю. Безопасность жизнедеятельности: учебник. 2-е изд. Ростов-на-Дону.: Феникс, 2007. С. 423.

[7] Кириллов В.А., Киселев В.В. Безопасность информации: проблемы и пути их решения // Военная Мысль. 2004. №2. С. 16 — 20.

информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Особое значение вопрос обеспечения оперативной комплексной оценки состояния информационной безопасности приобретает в связи с проведением реформирования ВС РФ и переходом к межвидовым региональным группировкам войск (РГВ)[8]. В ходе реформирования целесообразно оптимизировать структуру и состав системы средств объективного контроля, в результате чего на систему объективного контроля могут быть возложены функции элемента обратной связи в системе управления войсками (СУВ) с целью оперативного информирования органов военного управления о своевременности, качестве и полноте проводимых войсками мероприятий по обеспечению информационной безопасности.

В настоящее время для сбора данных о состоянии информационной безопасности на объектах РГВ используют мобильные средства, стационарные центры и посты контроля по различным физическим полям, а также аппаратуру, установленную на авиационных носителях и космических аппаратах. Собранные разнородные данные по существующим линиям связи передаются в органы военного управления, где производится оценка состояния информационной безопасности как на отдельных объектах, так и по группировке в целом.

Недостатками используемых в настоящее время информационно-управляющих систем обеспечения оценки ИБ территориально рассредоточенных военных объектов и РГВ в целом являются:

недостаточная оснащенность подразделений и частей контроля средствами инструментального контроля ИБ и передачи его результатов;

отсутствие согласованного различными ведомствами, а в некоторых случаях и внутри них, методического обеспечения, позволяющего формировать единую (унифицированную) форму представления результатов оценки состояния ИБ объектов независимо от их количества, типа, а также от условий функционирования, количества и физической сущности их характеристик;

различные структуры, объемы и семантическое содержание передаваемых информационных потоков, что влечет необходимость использования значительного количества и различных типов аппаратно-программных комплексов (АПК), имеющих специфические характеристики для обработки каждого типа потоков;

большие временные затраты на передачу (сбор) измерительной информации, ее обновление из-за ограниченной пропускной способности линий связи и, как следствие, ограниченная пригодность результатов оценки и прогнозирования изменений состояния ИБ для своевременного формирования и осуществления управляющих воздействий с целью корректировки значений ее характеристик;

ограниченные возможности по одновременному представлению (отображению) результатов оценки состояния и динамичности изменений ИБ по всей совокупности разнородных контролируемых характеристик и, как следствие, низкая оперативность комплексной оценки взаимосвязи характеристик ИБ и точность выявления источников или причин ее изменений.

С проблемой информационного сопряжения и представления разнородных данных столкнулись и разработчики системы автоматизированного контроля состояния потенциально опасных объектов Российской Федерации в интересах обеспечения защиты от техногенных,

[8] Независимое военное обозрение. 2006 г. № 42.

природных и террористических угроз[9], попытавшиеся преодолеть различия в способах получения и представления разнородной информации в сопрягаемых системах за счет использования ограниченного перечня совпадающих, т.е. обязательно получаемых каждой из систем, характеристик состояния потенциально опасных объектов. Данный подход требует разработки и внедрения аппаратно-программных комплексов, имеющих специфические характеристики, использования большого количества широкополосных быстродействующих линий связи и в настоящее время является достаточно затратным, из-за чего его использование для оценки состояния ИБ в группировках войск нецелесообразно.

Другим подходом к преодолению проблем сопряжения и представления разнородной информации является создание многоуровневых и многофункциональных организационно-технических систем защиты информации[10]. Данный подход основывается на структуризации сложной предметной области, включающей разнородные и разноуровневые стационарные объекты, находящиеся во взаимосвязи друг с другом. Структурирование позволяет выявить различные элементы описания, необходимые и достаточные для представления определенного состояния ИБ стационарного объекта. При этом, данный подход не позволяет существенно сократить временные затраты на передачу значительного объема информации и требует разработки специального математического и программного обеспечения (СМПО), обеспечивающего унифицированное представление состояния ИБ объектов воинских формирований или региона в целом. В связи с вышеуказанным использование данного подхода для оценки ИБ группировок войск также не представляется целесообразным.

Таким образом, задача обеспечения своевременной передачи, обработки и оценки значительного количества разнородной информации о состоянии информационной безопасности региональной группировки войск является актуальной и требует незамедлительного решения.

Данная проблема может быть преодолена за счет разработки и внедрения в СМПО СУВ и систем объективного контроля совокупности унифицированных, последовательно выполняемых вычислительных и логических процедур, обеспечивающих оценку и компактное отображение состояния ИБ объекта или РГВ в целом, ее изменений под воздействием внутренних и внешних факторов.

Предлагаемая авторами методика комплексной оценки состояния и изменений информационной безопасности предназначена для использования в СМПО средств СУВ и системы объективного контроля в качестве унифицированного модуля оценки соответствия установленным нормам фактических значений характеристик ИБ контролируемых объектов.

По мнению авторов, практическая реализация предлагаемой методики обеспечит:

оценку соответствия установленным нормам фактических значений характеристик ИБ контролируемых объектов и РГВ, в масштабе времени, близком к реальному;

снижение уровня требований по пропускной способности к каналам передачи данных о результатах контроля;

---

[9] Патент на изобретение, Россия, № 2243554, МПК G 01 N 33/00, 2004. Система автоматизированного контроля состояния потенциально опасных объектов Российской Федерации в интересах обеспечения защиты от техногенных, природных и террористических угроз.

[10] Герасименко В.Г., Донцов Г.Ю., Королёв А.А., Лаврухин Ю.Н. Основные принципы и результаты структурирования предметной области «Защита информации» // Общесистемные вопросы защиты информации: Коллективная монография / под ред. Сухарева Е.М.. Кн.1. М.: Радиотехника, 2003. С.20 — 36.

единообразное (унифицированное) отображение результатов контроля независимо от типа контролируемых объектов, количества и физической сущности их характеристик.

Целью разработки методики является повышение оперативности комплексной оценки соответствия состояния ИБ контролируемых объектов и РГВ установленным нормам, его изменений по результатам различных видов объективного контроля и полноты (эффективности) выполнения подразделениями и частями мероприятий по обеспечению требований по ИБ.

Решение поставленной задачи обеспечивается введением в состав СМПО, используемого органами военного управления и системами объективного контроля, унифицированных процедур формирования результатов оценки состояния ИБ отдельных объектов контроля и РГВ в целом, а именно:

формированием в аппаратно-программных комплексах центров обработки и управления базы данных по характеристикам средств контроля и ИБ районов дислокации войск;

созданием в аппаратно-программных комплексах центров обработки и управления до начала сбора данных правил формирования заданий средствам объективного контроля, протоколов результатов комплексной оценки состояния ИБ объектов, районов дислокации войск, а также локальных баз данных по характеристикам объектов, контролируемых конкретным видом объективного контроля, и единых унифицированных правил формализации результатов оценки состояния ИБ объектов;

передачей по линиям связи данных о результатах оценки состояния ИБ объектов, а не всех массивов данных, полученных средствами объективного контроля при проведении измерений;

использованием в центре обработки и управления правил формирования протоколов результатов комплексной оценки состояния ИБ объектов и РГВ в целом.

На рисунке 1 представлена схема процесса комплексной оценки состояния ИБ региональной группировки войск.

В соответствии с предлагаемой методикой до начала сбора данных в РГВ, состоящей из воинских формирований, включающих объекты контроля, в центре обработки и управления формируют:

базу данных, содержащую идентификаторы ID={IS, IO, IY}, где IS={$IS_з$} — идентификаторы средств контроля, IO={IO_i}, i=1,...,I — идентификаторы объектов контроля и IY ={y_{ij}} - идентификаторы контролируемых характеристик объектов;

последовательность моментов времени {t_n}, n=1,...,N_η передачи результатов оценки состояния ИБ объектов от средств объективного контроля в центр обработки и управления, при этом $t_n = t_0 + \eta\Delta_\eta$, где t_0 — время начала контроля, Δ_η — заданный для η-того средства интервал времени формирования результатов оценки состояния ИБ объектов, значение которого может варьироваться в зависимости от динамики изменения состояния оперативной обстановки и ИБ объектов контроля;

совокупность правил, обеспечивающих:

отображение содержания принятых от средств контроля данных о результатах оценки состояния ИБ объектов контроля;

формирование протоколов результатов комплексной оценки состояния ИБ объектов.

На каждом средстве объективного (инструментального) контроля формируют локальную базу данных, содержащую:

номер η средства контроля, номера $\{j\}_{i\eta}$ назначенных центром обработки и управления характеристик, по которым на η-том средстве

производят оценку соответствия состояния ИБ *i*-того объекта контроля установленным нормам по ИБ;

матрицу $D_i = (y_{ij}^H, y_{ij}^B)$ нижних и верхних границ интервалов

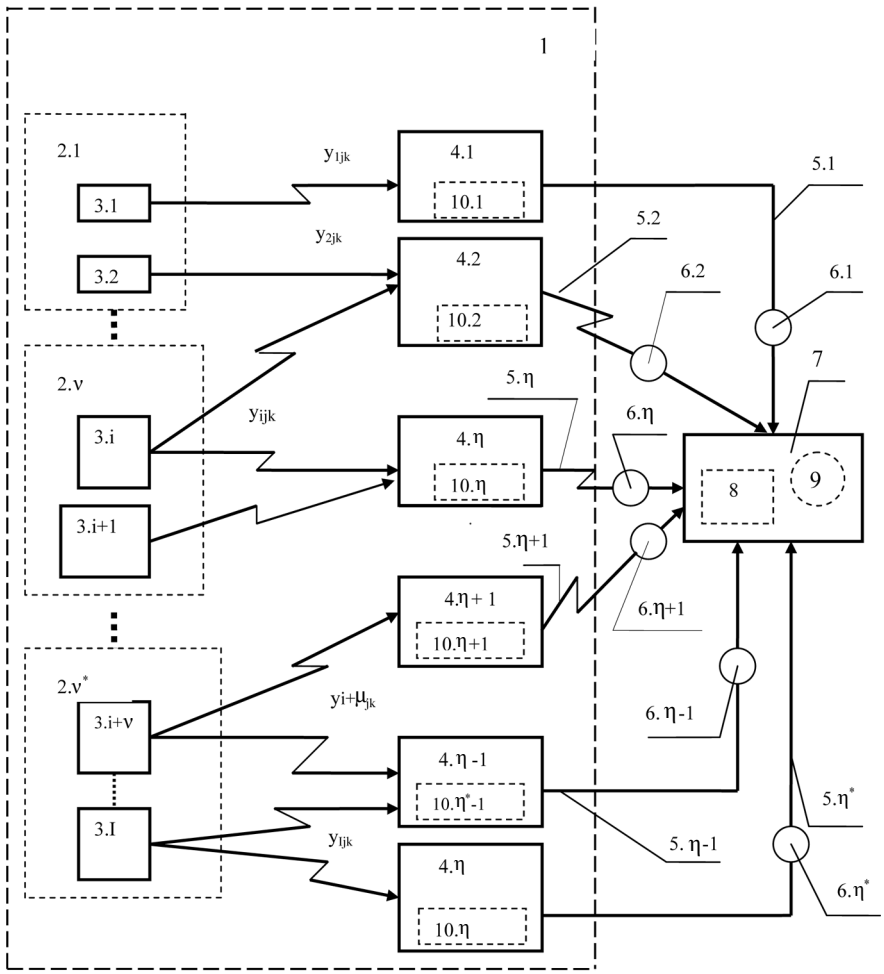

Рис. 1. Схема процесса комплексной оценки состояния информационной безопасности региональной группировки войск

*1 – региональная группировка войск;
2.1...2.ν — воинские формирования;
3.1...3.I — объекты контроля;
4.1...4.η — средства объективного контроля;
5.1...5.η — линии связи;
6.1...6.η — данные о результатах оценки состояния ИБ объектов контроля;
7 – центр обработки и управления;
8 – база данных;
9 –протокол результатов комплексной оценки состояния ИБ РГВ;
10.1...10.η — локальные базы данных.

допустимых значений для каждой из контролируемой конкретным средством совокупности характеристик $\{\hat{y}_{ij}\}$, по которым производят оценку соответствия состояния ИБ объекта контроля установленным нормам по ИБ;

словарь терминов, которые используются для формирования текстовой части табличной формы $T=\{T_1,T_2\}$ унифицированных протоколов результатов оценки состояния ИБ объектов контроля (ОК). При этом T_1 — текстовая часть единой для всех средств формы, которая предназначена для отображения времени окончания измерений, идентификаторов (наименований) средств контроля, номеров объектов контроля и координат местоположения объектов и средств объективного контроля; T_2 — текстовая часть табличной формы, содержание которой формируется в зависимости от результатов контроля характеристик объектов контроля конкретным средством контроля (в содержание T_2 могут включаться рекомендации по устранению нарушений установленных норм по ИБ).

совокупность унифицированных правил, обеспечивающих преобразование собранных средствами контроля разнородных данных для вычисления значений характеристик, по которым оценивают состояние ИБ объектов контроля (ОК), формирование и передачу в центр обработки и управления сообщений, формализованных результатов оценки состояния ИБ объектов контроля.

В соответствии с предлагаемой методикой в каждом заданном временном интервале с момента времени $t=t_0$ начала сбора разнородных данных $Y_i=\{y_{ij}\}$ о состоянии ИБ объекта, имеющего номер i, проводят n_j^* измерений значений каждого из назначенных для контроля параметров. Фиксируют время окончания измерений $t_f \in [t_0, t_к]$. Затем в интервале $t_f < t < t_к$ в соответствии с введенными до начала сбора данных правилами, по измеренным значениям y_{ijn}, $n=1, ..., n_j^*$ формируют совокупность $\{\hat{y}_{ij}\}|\ \hat{y}_{ij}=f_j(y_{ijn})$ оцененных значений параметров.

Далее проверяют выполнение условий $y_{ij}^H \le \hat{y}_{ij} \le y_{ij}^B$ и вычисляют величины $\delta_{ij}^0, \delta_{ij}^1$ являющиеся признаками и мерой несоответствия или соответствия оцененных значений параметров объекта контроля допустимым значениям:

$$\delta_{ij}^0 = \begin{cases} \left| \dfrac{\hat{y}_{ij}}{y_{ij}^B} \right|, & \hat{y}_{ij} > y_{ij}^B \\ \left| \dfrac{\hat{y}_{ij}}{y_{ij}^H} \right|, & \hat{y}_{ij} < y_{ij}^H \end{cases} \qquad (1)$$

$$\delta_{ij}^1 = 1,\ y_{ij}^H \le \hat{y}_{ij} \le y_{ij}^B.$$

Для удобства, величины $\delta_{ij}^0, \delta_{ij}^1$ далее в тексте интерпретируются как признаки соответствия оцененных значений параметров объекта контроля допустимым значениям.

Затем формируют матрицу δ_i состояния объекта контроля, элементам которой присваивают вычисленные значения признаков соответствия

$\delta_i = \left(\delta_{ij}^0, \delta_{ij}^1\right)_{1\times j}^*$, имеющую структуру и размерность матрицы Y_i контролируемых параметров объекта, которые группируют по видам $\nu=1, ...,\nu^*$ контроля, соблюдая при этом общую нумерацию. Порядок расположения сгруппированных по видам контроля значений признаков соответствия в матрице δ_i представлен в таблице 1. Наличие в матрице значений элементов, равных нулю, означает, что в заданном временном интервале параметры с номерами, соответствующими номерам элементов матрицы, содержащих ноль, не контролируются.

Таблица 1

Матрица состояния информационной безопасности объекта контроля в момент времени окончания измерений $t_{f=1}$

δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_{14}	δ_{15}	δ_{16}	δ_{17}	δ_{18}	δ_{20}	δ_{21}	δ_{22}	δ_{23}	δ_{24}	δ_{25}
1	1	0,875	1	1	1,25	1	1	1	1,167	1,25	1	1	1,15	1	1	1	1

Используя матрицу δ_i состояния в $P(\rho_{ij}, \theta_{ij})$ — полярной системе координат формируют и отображают цветографическую форму (рис.2), которая содержит результаты допусковой оценки каждого из контролируемой совокупности параметров, формализованные в виде фигуры, ограниченной замкнутой ломаной линией, соединяющей множество $M_i=\{M_i^1, M_i^0\}$ меток, координаты расположения которых формируют, присваивая значениям ρ_{ij} полярных радиусов, вычисленные значения признаков δ_{ij} соответствия оцененных и допустимых значений контролируемых параметров и вычисляя значения θ_{ij} углов поворота радиусов относительно полярной оси.

Формализацию осуществляют по следующим, унифицированным для всех контролируемых параметров правилам.

В случаях, если оцененные значения $\hat{y}_{ij}$ находятся в интервалах допустимых значений, в полярной системе координат фиксируют метки ($M_i^1 \in M_i$) с координатами (ρ_{ij}, θ_{ij}) на окружности, где $\rho_{ij}=\delta_{ij}^1=1$ — радиус и θ_{ij} — угол его поворота относительно полярной оси (рис.2). Значения углов θ_{ij} вычисляются по формуле:

$$\theta_{ij} = , \quad \frac{\theta}{\omega} j \qquad (2)$$

где $\theta = \frac{360^\circ}{j^*}$; ω — градусная мера радиана.

В случаях, если оцененные значения $\hat{y}_{ij}$ находятся вне интервалов допустимых значений, фиксируют метки ($M_i^0 \in M_i$) с координатами (ρ_{ij}, θ_{ij}), не находящиеся на окружности единичного радиуса, так как $\rho_{ij}=\delta_{ij}^0$, а $\delta_{ij}^0 \neq 1$. Все зафиксированные метки последовательно, начиная с первой, соединяют линией. При этом формируются и при визуальном отображении наблюдаются изломы линии в местах расположения меток, не находящихся на окружности единичного радиуса (рис. 2).

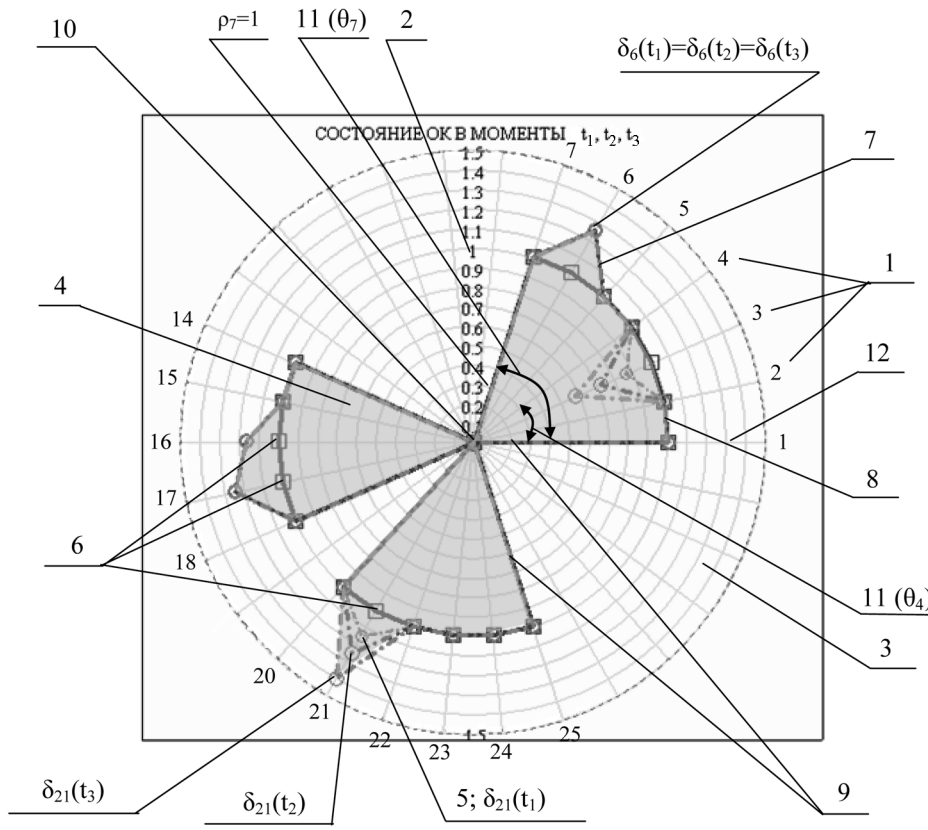

Рис. 2. Совмещенные цветографические образы состояния информационной безопасности объекта из состава региональной группировки войск

1 — номера контролируемых параметров;
2 — шкала для определения значений признаков соответствия оцененных и допустимых значений контролируемых параметров объекта контроля;
3 — полярная система координат;
4 — цветографический образ;
5 — метки значений признаков соответствия оцененных и допустимых значений контролируемых параметров в моменты времени t_1, t_2, t_3;
6 — метки эталонных значений признаков соответствия оцененных и допустимых значений контролируемых параметров;
7 — линия границы фигуры образа состояния объекта;
8 — линия границы фигуры эталонного образа;
9 — полярные радиусы;
10 — полюс полярной системы координат;
11 — полярные углы;

Количество и номера всех зафиксированных меток на окружности и вне ее соответствуют числу j^* и номерам контролируемых параметров объекта контроля. Направление, относительные величины изломов линии, формируют по результатам анализа ситуации, при которой за-

фиксировано отклонение оцененного значения параметра от нижней $\hat{y}_{ij} < y_{ij}^{H}$ или верхней $\hat{y}_{ij} > y_{ij}^{B}$ границы допуска.

Сформированную фигуру интерпретируют как цветографический образ (ЦГО) состояния объекта контроля в момент t_f, f=1, ..., f^* окончания измерений. В общем случае количество моментов t_f соответствует количеству моментов $t_к$, к=1, ...,$к^*$ окончания заданных интервалов времени получения данных о результатах комплексного контроля состояния многопараметрического объекта.

Для оперативного визуального выявления фактов соответствия и несоответствия фактического состояния ИБ объекта установленным нормам в этой же системе координат формируют фигуру, граничная линия которой соединяет расположенные на окружности f^* меток ($M_i^Э$) другого типа с координатами (ρ_{ij}=1, θ_{ij}) и интерпретируют ее как эталонный цветографический образ состояния ИБ объекта контроля, который соответствует случаю, когда значения всех контролируемых параметров находятся в границах допусков, а значения признаков соответствия равны единице. Матрица значений признаков соответствия для формирования эталонного ЦГО имеет размерность и структуру матрицы контролируемых параметров.

Далее после формирования эталонного ЦГО совмещают цветографические образы, сформированные в предыдущих и в последнем (текущем) заданных временных интервалах. Фиксируют по изменениям координат меток, имеющих одинаковые номера в совмещаемых ЦГО, факты наличия, тенденции, значения и величины изменений признаков соответствия параметров объекта.

Из значений признаков соответствия и моментов окончания измерений с учетом последовательности их получения формируют временные ряды $\{\delta_{ij}(t), t\}$, по содержимому которых для более точного определения формы, числовых характеристик тенденций изменений формируют модель изменения признаков во времени $\delta_{ij}(t)=F_j(a_0, a_1, ... t)$, где $a_0, a_1, ...$ — коэффициенты модели, вычисленные по значениям временного ряда; $t=\{t_f\}$- совокупность моментов времени окончания измерений в заданных временных интервалах; F_j — оператор, определяющий форму зависимости.

Сформированные временные ряды при необходимости используют как исходные данные для определения динамических и корреляционных свойств контролируемых параметров при выявлении причин, а также при определении возможных последствий изменения состояния объекта контроля. Для этого экстраполируют, получают точечную $\hat{y}_{ij}^{KP}$ и интервальную $\hat{y}_{ij}^{KP} \pm \sigma_{ij}$ оценки значений параметров объекта, при которых может возникнуть критическая ситуация, и фиксируют моменты времени t_{ij}^{KP} прогнозируемого достижения этих значений[11,12].

С учетом результатов комплексной оценки состояния ИБ и прогнозирования изменения значений ее характеристик принимаются решения по использованию сил и средств объективного контроля, а также подразделений, предназначенных для замысла операции, устранения (профилактики) нарушений установленных норм ИБ.

Зная количество зафиксированных случаев нарушений $\sum_j^{\delta_{ij}} \mid \delta_{ij} \neq 1$, можно определить значения полноты (эффективности) E_i проведенных

[11] Дж. Бендат, А. Пирсол. Прикладной анализ случайных данных. М.: Мир, 1989. С. 106 — 117.

[12] Елисеева И.И., Юзбашев М.М. Общая теория статистики. М.: Финансы и Статистика, 1995. С. 245 — 256, С. 304 — 313.

мероприятий по выполнению норм ИБ на конкретном объекте или в РГВ в целом.

$$\Gamma_{\nu} = 1 - \left(\frac{\sum_{j} \delta_{j}}{J_{\nu}} \right) \qquad (3)$$

Возможность реализации предлагаемой методики иллюстрируется следующим примером. Предположим, что в моменты времени t_1, t_2, t_3 окончания заданных временных интервалов необходимо оценить состояние информационной безопасности пространственно-распределенного объекта (далее по тексту объект контроля) по измеренным значениям 18-ти разнородных параметров, наименования, идентификаторы и допустимые значения которых приведены в таблице 1. При этом полагаем, что параметры объекта контроля, имеющие номера с 8 по 13, 19 и с 26 по 30 на заданных временных интервалах не контролировались, и по этой причине их наименования, идентификаторы и допустимые значения в таблице 1 не приведены. Для рассматриваемого объекта контроля в заданных временных интервалах объективный контроль включает три вида контроля (контроль в инфракрасном диапазоне длин волн, радиоконтроль, оптический контроль), имеющих номера ν=1, 4, 6. Контролируемые параметры сгруппированы по видам контроля. Так при ведении контроля, имеющего номер ν=1, контролируются параметры с номерами j=1, ..., 7. При ведении контроля, имеющего номер ν=4, контролируются параметры с номерами j=14, ..., 18. При ведении контроля, имеющего номер ν=6, контролируются параметры с номерами j=20, ..., 25. В первом заданном временном интервале $\Delta t_1=[t_0,t_{\kappa=1}]$ после проведения и фиксации момента окончания измерений $t_{f=1}$, оценивания значения каждого контролируемого параметра, сравнения оцененных значений $\hat{Y}_j$ с допустимыми значениями $[Y_j^H, Y_j^B]$, преобразовывают результаты допусковой оценки путем вычисления значений признаков соответствия δ_j по правилам (1), формируют матрицу $\delta(t_1)$ состояния ИБ объекта контроля. Структура и содержание матрицы приведены в таблице 1. При этом элементы матрицы, имеющие номера, совпадающие с номерами неконтролируемых параметров, т.е. с 8 по 13, 19 и с 26 по 30, и содержащие нулевые значения, в таблице 1 не представлены.

Далее определяют значения углов θ_j по формуле (2).

В полярной системе координат по правилам (1) формируют и отображают ЦГО (рис. 2), соответствующий образу состояния ИБ объекта контроля в момент $t_{f=1}$ окончания измерений во временном интервале Δt_1, используя при этом в качестве исходных данных значения признаков соответствия из таблицы 2.

Далее во втором и в третьем временных интервалах выполняют ту же последовательность действий и формируют в той же системе координат ЦГО, соответствующие образу состояния ИБ объекта контроля в моменты $t_{f=2}$, $t_{f=3}$ окончания измерений во временных интервалах Δt_2, Δt_3, используя при этом в качестве исходных данных значения признаков соответствия из таблиц 3 и 4.

Определяют по изменениям координат расположения меток с одинаковыми номерами в совмещаемых образах (рис. 2) факты несоответствия оцененных допустимым значениям контролируемых параметров и факты наличия изменений значений признаков соответствия, относительные величины, тенденции (направления) их изменений, а именно:

тенденцию к уменьшению значений признаков соответствия $\delta_3(t_1) > \delta_3(t_2) > \delta_3(t_3)$;

Таблица 2

Наименования, идентификаторы, оцененные и допустимые значения параметров состояния информационной безопасности объекта

Наименование контролируемых параметров пространственно-разнесенного объекта	Идентификаторы оцененных значений	Минимально и максимально допустимые значения параметров объекта		Оцененные значения проконтролированных параметров		
		Идентификаторы	Значения	в момент t_1	в момент t_2	в момент t_3
Количество источников ИК-излучений в составе объекта, шт	$\hat{Y}_1$	$Y_1^н \dots Y_1^в$	2…3	3	3	3
ИК-контраст первого элемента объекта относительно фона	$\hat{Y}_2$	$Y_2^н \dots Y_2^в$	0,2…0,3	0,25	0,25	0,25
ИК-контраст второго элемента объекта	$\hat{Y}_3$	$Y_3^н \dots Y_3^в$	0,2…0,3	0,175	0,143	0,114
Азимут центра второго элемента объекта относительно центра первого элемента, град	$\hat{Y}_4$	$Y_4^н \dots Y_4^в$	15	15	15	15
ИК-контраст третьего элемента объекта относительно фона	$\hat{Y}_5$	$Y_5^н \dots Y_5^в$	0,2…0,3	0,27	0,27	0,27
Расстояние между центрами первого и третьего элементов объекта, м	$\hat{Y}_6$	$Y_6^н \dots Y_6^в$	15…20	25	25	25
Азимут центра третьего элемента объекта относительно центра первого элемента, град	$\hat{Y}_7$	$Y_7^н \dots Y_7^в$	45	45	45	45
Количество источников радиоизлучений (ИРИ) в составе объекта, шт	$\hat{Y}_{14}$	$Y_{14}^н \dots Y_{14}^в$	2	2	2	2
Значение центральной несущей частоты первого ИРИ, ГГц	$\hat{Y}_{15}$	$Y_{15}^н \dots Y_{15}^в$	2,5…2,6	2,55	2,55	2,55
Ширина спектра сигнала первого ИРИ, кГц	$\hat{Y}_{16}$	$Y_{16}^н \dots Y_{16}^в$	250…300	350,1	350,1	350,1
Значение центральной несущей частоты второго ИРИ, ГГц	$\hat{Y}_{17}$	$Y_{17}^н \dots Y_{17}^в$	1,25…1,5	1,875	1,875	1,875
Ширина спектра сигнала второго ИРИ, кГц	$\hat{Y}_{18}$	$Y_{18}^н \dots Y_{18}^в$	200…250	233	233	233
Количество контрастирующих элементов изображения объекта в видимом диапазоне длин волн, шт	$\hat{Y}_{20}$	$Y_{20}^н \dots Y_{20}^в$	2…3	3	3	3
Контраст первого элемента объекта относительно фона	$\hat{Y}_{21}$	$Y_{21}^н \dots Y_{21}^в$	0,3…0,35	0,403	0,438	0,49
Контраст второго элемента объекта относительно фона	$\hat{Y}_{22}$	$Y_{22}^н \dots Y_{22}^в$	0,3…0,35	0,33	0,33	0,33
Контраст третьего элемента объекта относительно фона	$\hat{Y}_{23}$	$Y_{23}^н \dots Y_{23}^в$	0,3…0,35	0,345	0,345	0,345
Азимут центра второго элемента объекта относительно центра первого элемента, град	$\hat{Y}_{24}$	$Y_{24}^н \dots Y_{24}^в$	35	35	35	35
Азимут центра третьего элемента объекта относительно центра первого элемента, град	$\hat{Y}_{25}$	$Y_{25}^н \dots Y_{25}^в$	82	82	82	82

Таблица 3

Матрица состояния информационной безопасности объекта контроля в момент времени окончания измерений $t_{f=2}$

δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_{14}	δ_{15}	δ_{16}	δ_{17}	δ_{18}	δ_{20}	δ_{21}	δ_{22}	δ_{23}	δ_{24}	δ_{25}
1	1	0,714	1	1	1,25	1	1	1	1,167	1,25	1	1	1,25	1	1	1	1

Таблица 4

Матрица состояния информационной безопасности объекта контроля в момент времени окончания измерений $t_{f=3}$

δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_{14}	δ_{15}	δ_{16}	δ_{17}	δ_{18}	δ_{20}	δ_{21}	δ_{22}	δ_{23}	δ_{24}	δ_{25}
1	1	0,57	1	1	1,25	1	1	1	1,167	1,25	1	1	1,4	1	1	1	1

факты не изменяющихся во времени значений признаков соответствия $\delta_6(t_1) = \delta_6(t_2) = \delta_6(t_3)$, $\delta_{16}(t_1) = \delta_{16}(t_2) = \delta_{16}(t_3)$, $\delta_{17}(t_1) = \delta_{17}(t_2) = \delta_{17}(t_3)$;

тенденцию к увеличению значений признаков соответствия $\delta_{21}(t_1) < \delta_{21}(t_2) < \delta_{21}(t_3)$.

Анализ данных позволяет сделать вывод о том, что в течение трех заданных временных интервалов на объекте контроля выявлено 5 нарушений норм информационной безопасности.

Подставляя количество зафиксированных случаев нарушений в выражение (3), определяем значение полноты (эффективности) проведенных мероприятий по выполнению норм ИБ на объекте контроля:

$$D_3 = 1 - \left(\frac{5}{18}\right) = 0,72$$

Т. е. в результате оценки состояния ИБ на объекте контроля установлено, что в соответствии с требованиями к моменту времени t_3 выполнено только 72 % мероприятий по обеспечению ИБ.

Аналогичным образом могут быть определены и значения полноты (эффективности) проведенных мероприятий по выполнению требований по ИБ для РГВ в целом.

По мнению авторов, использование предлагаемой методики позволит:

обеспечить комплексную оценку соответствия состояния ИБ объектов и РГВ в целом установленным нормам в масштабе времени, близком к реальному;

снизить уровень загрузки используемых и имеющих ограниченную пропускную способность линий связи;

исключить необходимость разработки и применения СМПО сопряжения различных ведомственных форматов при интеграции разнородных данных;

обеспечить унификацию и компактность представления результатов оценки состояния ИБ контролируемых РГВ и изменений значений их характеристик, независимо от их количества и физической сущности;

обеспечить своевременное принятие решений органами государственного и военного управления по использованию сил и средств объективного контроля состояния ИБ, а также подразделений, предназначенных для замысла операции и устранения (профилактики) нарушений установленных норм по ИБ.