ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

О.М. Булгаков,
доктор технических наук, профессор

В.В. Стукалов,
кандидат технических наук, Воронежский институт Правительственной связи (филиал) Академии ФСО России

Е.А. Кучмасов,
ФКУ «Главный центр связи и защиты информации МВД России»

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛИ НАДЕЖНОСТИ ОРГАНИЗАЦИОННОГО КОМПОНЕНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

PRINCIPLES OF CREATING OF RELIABILITY MODELS FOR OBJECT INFORMATION DATA PROTECTION SYSTEM ORGANIZATIONAL COMPONENT

Показана возможность применения моделей оценки надежности технических систем для анализа надежности организационного компонента системы защиты информации объекта информатизации. В результате декомпозиции организационного компонента выделены четыре его функциональные подсистемы, для каждой из которых приведены аналитические выражения для расчета вероятности отказа.

The possibility of assessing the reliability of technical systems for the analysis of the reliability of the organizational component of the information object information protection system is demonstrated. Due to the decomposition of the organizational component assigned four functional subsystems, each of which provides analytical expressions to calculate the probability of failure.

Как правило, при оценке защищенности информации, проводимой с целью анализа эффективности системы защиты информации (СЗИ) какого-либо объекта информатизации, не рассматриваются вопросы надежности защиты информации. Это связано с тем, что в настоящее время не существует моделей надежности, с одной стороны, со-

гласующихся с общими подходами построения моделей надежности технических систем, а с другой — учитывающих специфику СЗИ. Разработанные модели надежности технических систем по ряду причин неприменимы к СЗИ, таким образом, вопрос о разработке модели надежности СЗИ является важной и актуальной задачей.

Схемы надежности, представляемые последовательно-параллельными соединениями элементов с известными количественными характеристиками надежности, широко применяются при построении моделей надежности сложных технических систем [1]. Однако такие схемы достаточно редко применяются для анализа систем защиты информации ввиду проблем детализации структуры объектов (декомпозиции) и четкого выделения элементов схемы и их взаимосвязей.

Рассмотрим структурную схему организационного компонента (ОК) СЗИ (рис. 1).

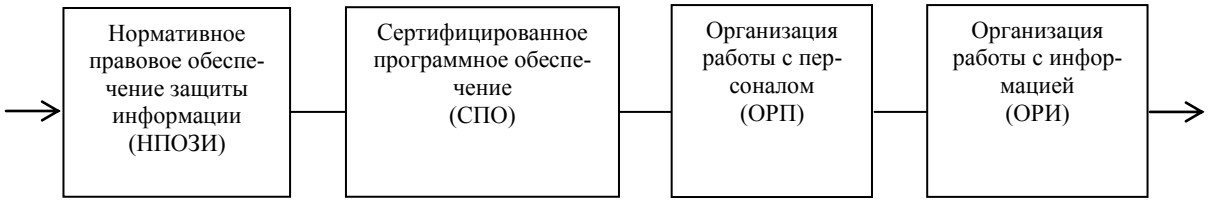


Рис. 1. Обобщенная схема надежности ОК СЗИ

При параллельном соединении системных элементов в схеме надежности отказ системы наступает лишь при одновременном отказе всех элементов системы, а при последовательном — при выходе из рабочего состояния хотя бы одного из них [1]. Будем считать фактором отказа (аргументом вероятности отказа в некоторый фиксированный момент времени) интенсивность *I* вредоносного воздействия на СЗИ, направленного на её преодоление или вывод из строя. В нашем случае выход из строя одного из средств (способов) защиты приводит к отказу всего компонента в целом. Каждое из направлений не может функционировать вне зависимости от работоспособности трех других. Отсюда можно сделать вывод, что все четыре направления организационных мер защиты информации, как одного из компонентов СЗИ в целом на схеме ее надежности должны быть соединены последовательно (рис.1).

Тогда вероятность безотказной работы ОК СЗИ:

$$P_{раб} = P_{НПОЗИ} \cdot P_{СПО} \cdot P_{ОРП} \cdot P_{ОРИ}\ , \qquad (1)$$

где $P_{раб}$ — вероятность безотказной работы ОК СЗИ;

$P_{НПОЗИ}$, $P_{СПО}$, $P_{ОРП}$, $P_{ОРИ}$ — вероятности безотказной работы соответствующих направлений ОК СЗИ: нормативного правового обеспечения, сертифицированного программного обеспечения, организации работы с персоналом, организации работы с информацией.

Рассмотрим подробно состав каждого из способов защиты и построим схему надежности ОК СЗИ с учетом декомпозиции (рис. 2).

Под отказом в теории надежности понимается событие, заключающееся в нарушении работоспособного состояния объекта или выхода функциональных параметров за допустимый диапазон значений [2]. Применяя данное определение к СЗИ, термин «отказ» можно трактовать как возникновение уязвимости в СЗИ в виде хотя бы одного канала утечки информации или появление возможности преодоления СЗИ злоумышленником.

Рассмотрим причины и механизмы возникновения отказа в различных подсистемах ОК СЗИ.

Применительно к нормативному правовому обеспечению защиты информации к таким причинам можно отнести:

- отсутствие утвержденной политики безопасности организации, разработанной в соответствии с требованиями регуляторов в области информационной безопасности;
- устаревание и нерегулярный мониторинг актуальности действующих НПА на международном, государственном и других уровнях;
- необоснованно долгие сроки вступления в силу вновь изданных (принятых) НПА и начало работы по новым требованиям и др.

Так как при выходе из строя хотя бы одной из составляющих частей данной подсистемы ОК СЗИ вероятность НСД к информации увеличится, но не приведет к отказу всей системы в целом, и каждая часть системы может функционировать вне зависимости от других, обеспечивая требуемый уровень защиты, то можно сделать вывод что все части рассмотренной подсистемы ОК СЗИ должны быть соединены параллельно (рис. 2).

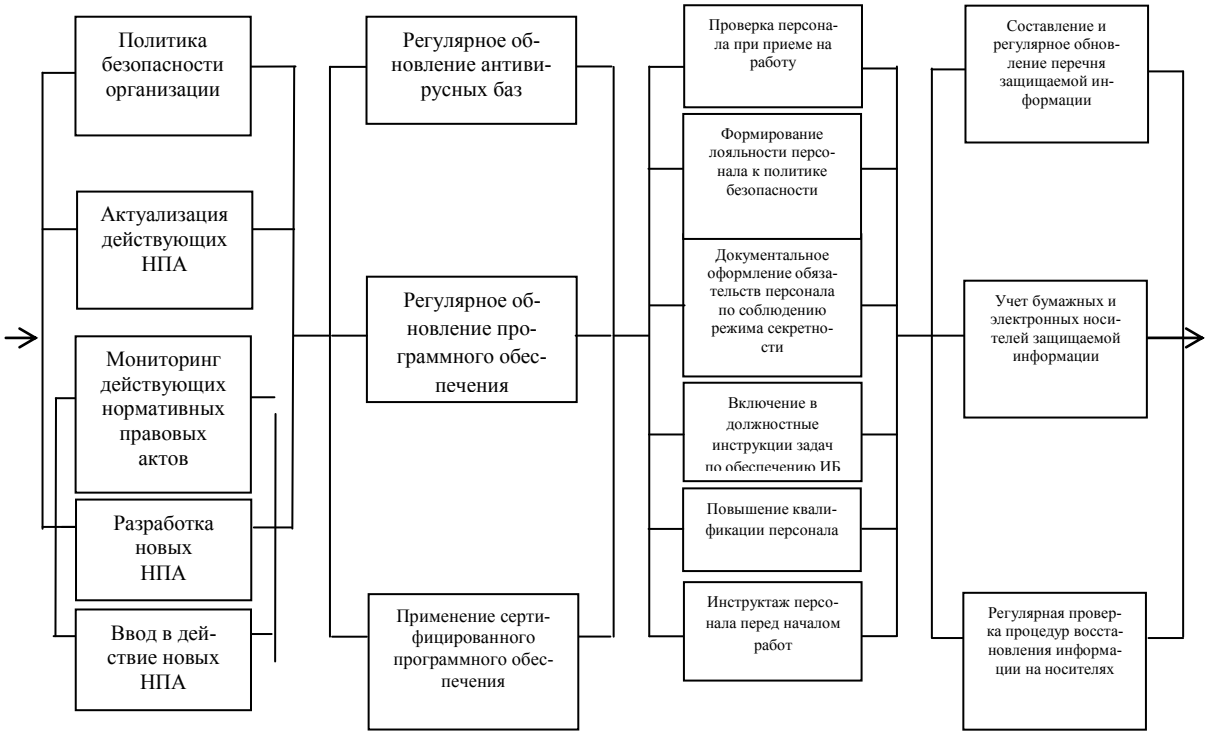


Рис. 2. Схема надежности организационного компонента системы защиты информации и его подсистем

Вероятность безотказной работы данной подсистемы:

$$P_{\text{НПОЗИ}_{\text{раб}}} = 1 - P_{\text{НПОЗИ}_{\text{отк}}} = 1 - P_{\text{ПБ}} \cdot P_{\text{АДНПА}} \cdot P_{\text{МДНПА}} \cdot P_{\text{РНПА}} \cdot P_{\text{ВНПА}}, \qquad (2)$$

где $P_{\text{ПБ}}, P_{\text{АДНПА}}, P_{\text{МДНПА}}, P_{\text{РНПА}}, P_{\text{ВНПА}}$ – вероятности отказа составляющих частей данного компонента в соответствии с рис. 2.

Очевидно, что все сомножители в (2) зависят от времени, причем на качественном уровне — сходно. Примерный вид зависимости от времени вероятности отказа рассматриваемой подсистемы показан на рис. 3.

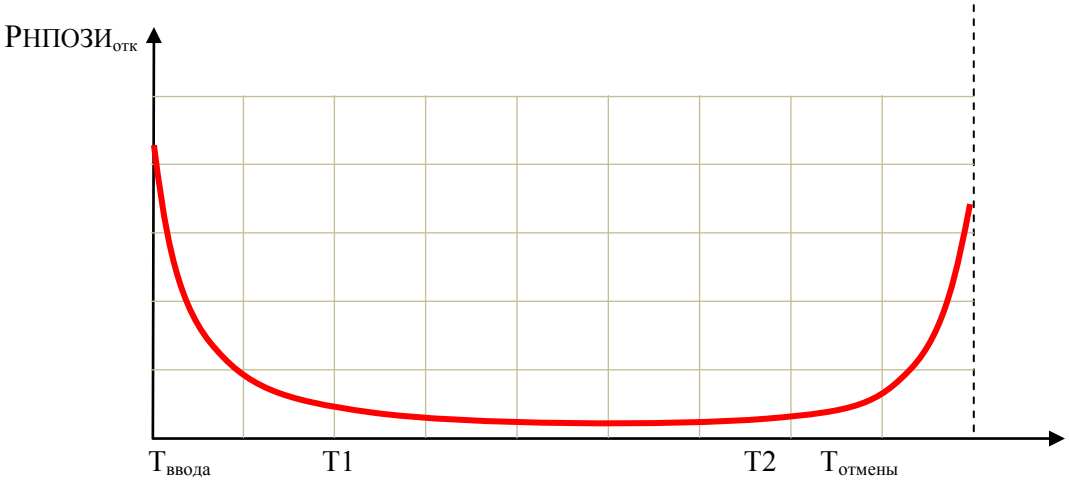


Рис. 3. Вероятность отказа подсистемы нормативного правового обеспечения защиты информации

За основу построения графика на рис. 3 взята классическая корытообразная кривая интенсивности отказов технических средств или радиокомпонентов [3], которую мы представили суммой графиков зависимостей:

$$P_{\text{НПОЗИотк}}(t) = P_{\text{НПО1}}(t) + P_{\text{НПО2}}(t), \text{ где}$$

$$P_{\text{НПО1}}(t) = P_{01} \cdot e^{-\frac{\gamma_1 \cdot t}{T_1}} \quad (3)$$

характеризует вероятность отказа системы при внедрении новой нормативно-правовой базы. Относительно большие значения $P_1(t)$ на начальном участке обусловлены тем, что в начале внедрения механизм реализации новых НПА недостаточно отработан, основные положения еще недостаточно изучены и восприняты всем персоналом, работающим в организации, и т.д.

В правой части выражения (3): T_1 — характерное время «приработки» нормативно-правовой базы, характеризующееся сроками изучения и внедрения в практическую деятельность НПА персоналом среднего уровня квалификации; $\gamma_1(t)$ — коэффициент, отражающий квалификацию и мотивацию персонала.

Количественно T_1 может определяться как время, за которое $P_1(t)$ уменьшается в e раз при $\gamma = 1$.

Функция

$$P_{\text{НПО2}}(t) = P_{02} \cdot e^{\frac{\gamma_2 \cdot t}{T_2}}, \quad (4)$$

описывает возрастание вероятности отказа системы при моральном устаревании нормативных правовых актов, регламентирующих политику безопасности организации. Этот процесс неизбежен при современном темпе технического развития, следствием которого является изменение задач обрабатываемой информации на контролируемом отрезке времени, что требует регулярного совершенствования политики информационной безопасности и её нормативной базы.

Здесь T_2 — характерное время устаревания нормативно-правовой базы, обусловленное изменением внешних правовых, технических и социально-экономических факторов; $\gamma_2(t)$ — коэффициент, характеризующий интенсивность отказов системы вследствие утраты актуальности действующих НПА и зависящий от квалификации персона-

ла в области нормативно-правового регулирования и структуры нормативного контроля в организации.

Для упрощения анализа на относительно коротком временном отрезке ($t_a \sim T_1$) можно полагать $\gamma_1(t)$ и $\gamma_2(t)$ не зависящими от времени, если в пределах t_a обе эти функции не претерпевают скачкообразных изменений.

Кривая на рис. 3 является упрощенной моделью, т.к. не учитывает модернизацию и актуализацию нормативно-правового обеспечения защиты информации, например, за счет ввода новых НПА и доработки уже существующих документов. Данные процессы могут быть описаны выражениями

$$P_1^*(T_{изм1}; t) = \sigma(t - T_{изм1}) \cdot [(P_1(T_{изм1})) \cdot (P_1(\Delta T_{изм1}) - \Delta P_1) + P_2(\Delta T_{изм1})], \quad (5)$$

$$P_2^*(T_{изм2}; t) = \sigma(t - T_{изм2}) \cdot [(P_1(T_{изм2})) \cdot (P_1(\Delta T_{изм2}) - \Delta P_2) + P_2(\Delta T_{изм2})] \quad (6)$$

и т.д. вплоть до некоторого $P_n^*(T_{измn}; t)$. Здесь $T_{изм1}, T_{изм2}, \ldots, T_{измn}$ — времена внесения изменений в НПА, ΔP_j, j=1,…, n — величины, характеризующие ожидания от внедрения j-го нормативного правового акта, $\sigma(t)$ — функция Хэвисайда [4].

$$P_1(\Delta T_{измj}) = e^{-\frac{\gamma 1 \cdot t}{\Delta T_{измj}}}, \quad (7)$$

$$P_2(\Delta T_{измj}) = e^{\frac{\gamma 2 \cdot t}{\Delta T_{измj}}}, \quad (8)$$

по аналогии с (3) и (4).

График, иллюстрирующий эти процессы, показан на рис. 4, а скорректированное выражение для вероятности отказа подсистемы нормативного правового обеспечения защиты информации:

$$P_{НПОЗИотк}(t) = P_{НПО1}(t) + P_{НПО2}(t) + \sum_{j=1}^{n} P_j^*(T_{измj}; t) \quad (9)$$

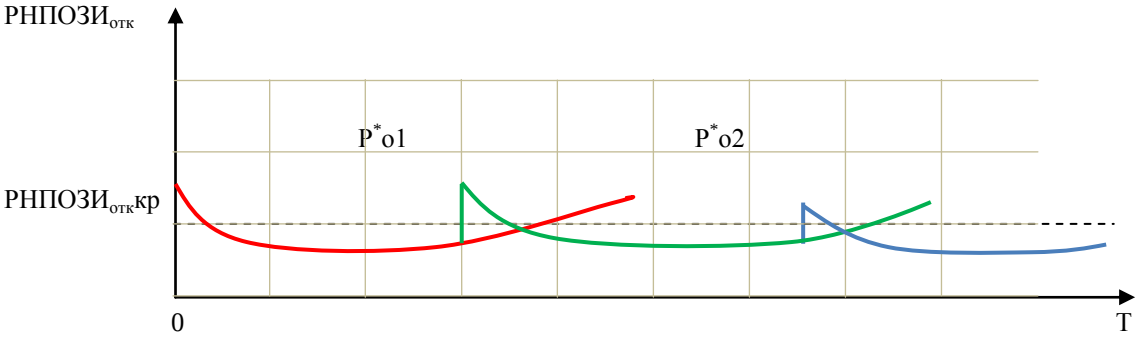


Рис. 4. Вероятность отказа подсистемы нормативно-правового обеспечения защиты информации при периодическом обновлении НПА

Пунктиром на рис. 4 показан приемлемый (допустимый) уровень вероятности отказа.

Как видно из графика на рис. 4, регулярные своевременные (до превышения $Рнпози_{отк}(t)$ приемлемого уровня) изменения нормативной базы обеспечивают поддержание требуемого уровня надежности подсистемы.

Применительно к механизму отказов СПО причинами отказа (деградации) будут: нерегулярное обновление антивирусных баз, версий операционных систем и прикладного программного обеспечения, использование в работе несертифицированного программного обеспечения, ошибки инсталляции программ, нерегулярная или некор-

ректная чистка реестров системы, нерегулярное удаление временных файлов прикладного программного обеспечения.

По аналогии с (2)

$$P_{\text{СПО}}=1-P_{\text{СПООтк}} \tag{10}$$

Рассмотрим случай, когда надежность СПО может быть охарактеризована посредством экспертизы:

$$P_{\text{СПООтк}}=\text{К}_{\text{СфПО}}\left(1-\frac{\Phi_{\text{НСПО}}}{\Phi_{\text{ПО}}}\right)+\text{К}_{\text{НСПО}}\frac{\text{К}_{\text{НСПО}}}{\Phi_{\text{ПО}}}\equiv P_{\text{СПООтк}}(0), \tag{11}$$

где $\text{К}_{\text{СфПО}}$, $\text{К}_{\text{НСПО}}$ — соответственно экспертные оценки вероятности отказов сертифицированного и несертифицированного программного обеспечения, используемого на объекте, $\Phi_{\text{НСПО}}$ и $\Phi_{\text{ПО}}$ – объем несертифицированного программного обеспечения и общий объём программного обеспечения соответственно.

Зависимость вероятности отказа СПО от времени:

$$P_{\text{СПООтк}}(t)=P_{\text{СПООтк}}(0)\cdot A\cdot\left[e^{-\frac{\alpha_1\cdot t}{T_1}}+e^{\frac{\alpha_2\cdot t}{T_2^*}}\right], \tag{12}$$

где A характеризует различные внутрисистемные факторы, обычно эргатической природы, влияющие на эффективность работы программного обеспечения; α_1 количественно отражает ошибки применения СПО на этапе его освоения, а также внедрения новых версий программных продуктов и т.д.; α_2 определяет устаревание компьютеров по отношению к программному обеспечению (системным требованиям), деградацию и моральное устаревание СПО.

График временной зависимости (12) аналогичен рис. 3.

Поддержание $P_{\text{СПООтк}}(t)$ ниже допустимого уровня обеспечивается регулярным обновлением СПО. По аналогии с (5) для *j*-го из *m* обновлений

$$P_j^{**}\left(T_{\text{обн}j};t\right)=\sigma(t-T_{\text{обн1}})\cdot\left[-P_{\text{СПО}}(0)_j\cdot P_j\left(\Delta T_{\text{обн}j}\right)+P_2\left(\Delta T_{\text{обн}j}\right)\right], \tag{13}$$

где $T_{\text{обн}j}$ — время ввода в работу нового программного обеспечения,

$$P_1\left(\Delta T_{\text{обн}j}\right)=e^{-\frac{\alpha 1\cdot t}{\Delta T_{\text{обн}j}}}, \tag{14}$$

$$P_2\left(\Delta T_{\text{обн}j}\right)=e^{\frac{\alpha 2\cdot t}{\Delta T_{\text{обн}j}}}. \tag{15}$$

Наряду с обновлением СПО уменьшению $P_{\text{СПООтк}}(t)$ способствует профилактическая работа системного администратора по переустановке операционной системы, прикладного программного обеспечения и утилит, дефрагментации логических дисков, очистке реестров и удалению неиспользуемых файлов и программ.

Этот процесс может быть отображен на графике ступенчатой функцией:

$$P_{\text{проф}k}^{**}\left(T_{\text{проф}k};t\right)=-Q_k\cdot\sigma\left(t-T_{\text{проф}k}\right), \tag{16}$$

где Q_k характеризует степень положительного воздействия k-го профилактического мероприятия.

Процессы, описываемые (13) и (16) графически представлены на рис. 5, а вероятность отказа СПО с их учетом:

$$P_{\text{СПООтк}}(t)=P\text{спо}(0)\cdot A\cdot\left[e^{-\frac{\alpha_1\cdot t}{T_1}}+e^{\frac{\alpha_2\cdot t}{T_2^*}}\right]+\sum_{j=1}^{m}P_j^{**}\left(T_{\text{обн}j};t\right)+\sum_{k=1}^{M}P_{\text{проф}j}^{**}\left(T_{\text{проф}j};t\right). \tag{11а}$$

Применительно к механизму ОРП под отказом понимается: недостаточно высокий уровень требований к персоналу при приёме на работу, низкий уровень квалификации работников, либо нерегулярное её повышение, отсутствие инструктажей перед началом проведения работ и др.

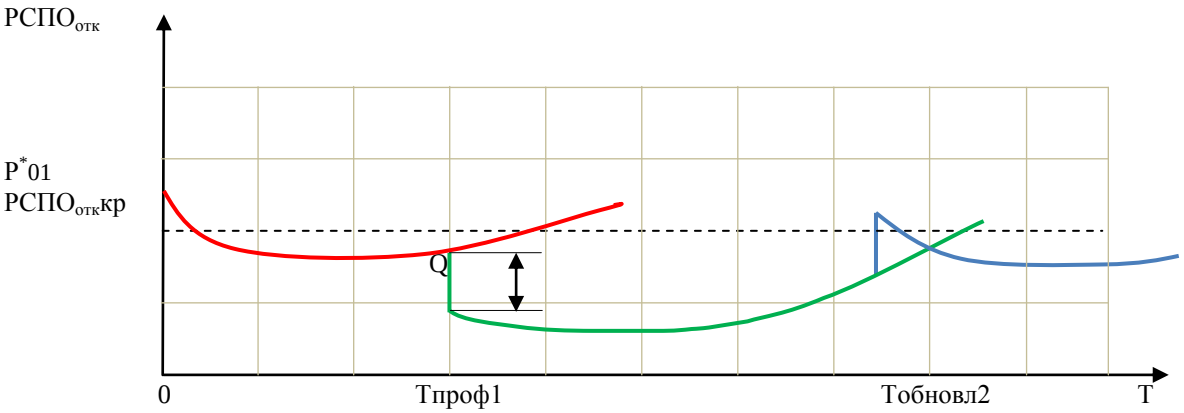


Рис. 5. Вероятность отказа подсистемы СПО при периодическом обновлении программного обеспечения

Приближенная статическая математическая модель отказа ОРП:

$$P_{\text{ОРПотк}}(0) = 1 - P_{\text{ОРП}}(0) = \frac{V_{\text{П}} \cdot K_{\text{ПП}} + (V_{\text{ОП}} - V_{\text{П}}) \cdot K_{\text{ПН}}}{V_{\text{ОП}}}, \quad (17)$$

где $V_{\text{П}}, V_{\text{ОП}}$ — объем персонала, прошедшего проверочные испытания и общий объем персонала соответственно, $K_{\text{ПП}}, K_{\text{ПН}}$ — экспертные оценки надежности персонала, соответственно прошедшего и непрошедшего проверочные испытания, пересчитанные в вероятность отказа СЗИ по его вине.

Зависимость вероятности отказа ОРП от времени:

$$P_{\text{ОРПотк}}(t) = P_{\text{ОРПотк}}(0) \cdot \text{В} \cdot \left[e^{-\frac{\omega_1 \cdot t}{T_1}} + e^{\frac{\omega_2 \cdot t}{T_2^*}} \right]. \quad (18)$$

Здесь В характеризует квалификацию персонала, соответствие занимаемой должности и т.п.; ω_1 отражает проблемы в работе подсистемы ОРП при приеме на работу новых сотрудников, назначении на другую должность и т.п.; ω_2 — количественный параметр, обусловленный необходимостью периодического повышения уровня квалификации сотрудников.

Уменьшению $P_{\text{ОРПотк}}(t)$ способствует своевременное повышение квалификации персоналом. Для *i*-го факта такого рода:

$$P^*_{\text{ПК}i}(T_{\text{ПК}i}; t) = -V \cdot \sigma(t - T_{\text{ПК}i}), \quad (19)$$

где V характеризует степень положительного эффекта от повышения квалификации.

При систематическом повышении квалификации персоналом, контроле со стороны руководства, своевременном приеме зачетов усредненное значение $P_{\text{ОРПотк}}(t)$ не будет превышать некоторый приемлемый (критический) уровень $P_{\text{ОРПотк кр}}$ (рис. 6).

Применительно к ОРИ причинами отказов могут быть: несвоевременное обновление перечня защищаемой информации, неправильное отнесение информации к разряду защищаемой, неправильный учет носителей защищаемой информации, утрата носителей защищаемой информации и т.д.

Вероятность отказа ОРИ в произвольный момент времени:

$$P_{\text{ОРИотк}}(t) = 1 - P_{\text{ОРИ}}(t) = P_{\text{ОРИотк}}(0) \cdot C \cdot \left[e^{-\frac{\psi_1 \cdot t}{T_1}} + e^{\frac{\psi_2 \cdot t}{T_2^*}} \right], \quad (20)$$

где

$$P_{\text{ОРИотк}}(0) = \frac{z_{\text{КНИ}} * \text{К}_{\text{КНИ}} + (z_{\text{НИ}} - z_{\text{КНИ}}) * \text{К}_{\text{НИ}}}{z_{\text{НИ}}}, \quad (21)$$

$z_{\text{КНИ}}, z_{\text{НИ}}$ — объем корректно учтенных носителей информации и общий объем носителей информации соответственно; $\text{К}_{\text{КНИ}}, \text{К}_{\text{НИ}}$ — экспертные оценки вероятности отказа корректно и некорректно учтенных носителей информации соответственно; C — коэффициент, характеризующий различные субъективные факторы, влияющие на корректность работы с различными носителями информации, применение перечней защищаемой информации на практике и т.д., например, традиционного или преемственного характера; ψ_1 отражает проблемы в работе подсистемы ОРИ при изменении и дополнении перечней защищаемой информации, изменении состава персонала, работающего с защищаемой информацией (например, после организационно-штатных мероприятий); ψ_2 количественное отражение необходимости своевременной корректировки перечня защищаемой информации, периодической ревизии всего объема информации, циркулирующей на объекте, с целью определения уровня корректности работы с ней персонала.

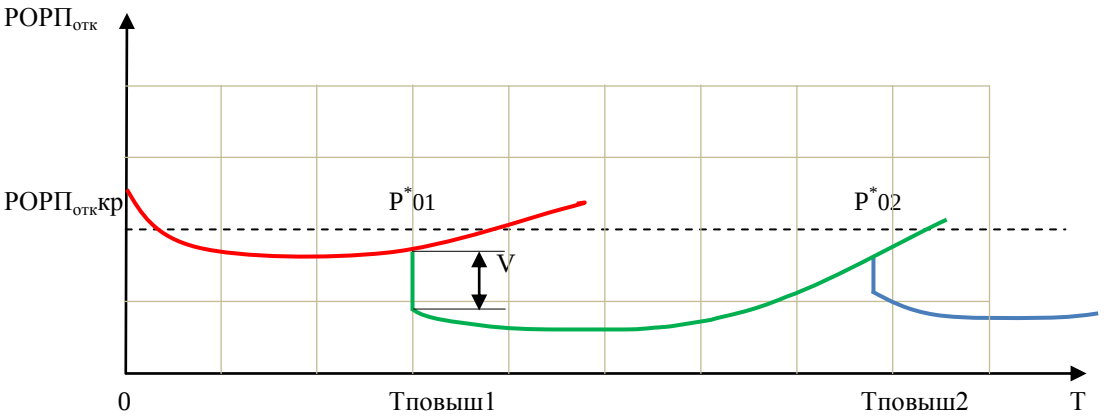


Рис. 6. Вероятность отказа подсистемы ОРП при периодическом обновлении программного обеспечения

Уменьшение $P_{\text{ОРИотк}}(t)$ за счет своевременных профилактических мер по корректировке перечней защищаемой информации, проведению разъяснительной работы с персоналом, приему у него зачетов по знанию документов, регламентирующих порядок работы с защищаемой информацией и т.д., может быть представлено в виде:

$$P^*_{\text{проф}.i}(T_{\text{проф}.i}; t) = -Y_k \cdot \sigma(t - T_{\text{проф}.i}), \quad (22)$$

где Y_k — оценка положительного воздействия профилактических мер.

При систематическом проведении профилактических мероприятий $P_{\text{ОРИотк}}(t)$ не будет превышать критическое значение аналогично $P_{\text{ОРПотк}}(t)$ на рис. 6.

Таким образом, организационный компонент системы защиты информации какого-либо объекта информатизации с помощью декомпозиции можно представить четырьмя подсистемами. Зависимости от времени вероятностей отказов выделенных подсистем ОК СЗИ: НПОЗИ, СПО, ОРП и ОРИ описываются идентично суммированием убывающей и возрастающей экспонент (рис. 3). Однако смысл и способы определения коэффициентов в показателях экспонент для вероятности отказа каждой подсистемы ОК СЗИ различны. Имеются различия и в описании воздействий на подсистемы с целью поддержания приемлемого уровня их надежности (рис. 4, 5, 6). Тем не менее, есть

основания утверждать, что вероятности отказов всех декомпозиционно выделенных компонентов ОК СЗИ как наиболее универсальных характеристик их надежности могут быть описаны одинаковым простым математическим аппаратом. Это позволяет существенно упростить оценки надежности организационного компонента и системы защиты информации в целом. На первый взгляд, не возникает трудностей с определением коэффициентов в выражениях (3)—(8) и (11)—(22). Временные параметры в знаменателях показателей экспонент и некоторые коэффициенты в числителе (например, ω_2, ψ_2) могут определяться разработчиком СЗИ или нормативными документами по ее эксплуатации и им подобными. Предполагается, что оставшаяся часть коэффициентов может быть установлена по экспертным оценкам.

В настоящее время теория надёжности технических систем разработана достаточно хорошо. Применение основных положений, терминов и определений теории надёжности технических систем в информационной безопасности открывает большие возможности для разработки моделей СЗИ, повышения достоверности оценок характеристик надёжности СЗИ и их отдельных компонентов, в особенности тех, на которые классические подходы теории надёжности технических систем ранее не распространялись. Предложенные нами модели надежности организационного компонента СЗИ и его подсистем показывают, что применение к системам защиты информации методов прогнозирования и оценки надежности технических систем расширяет базу для создания алгоритмов и методик анализа надёжности СЗИ, выбора эксплуатационных показателей их качества.

ЛИТЕРАТУРА

1. Баранова А.В., Ямпурин Н.П. Основы надежности электронных средств. — М.: Академия, 2010. — 234 с.

2. Острейковский В. А. Теория надежности. — М.: Высшая школа, 2003. — 457 с.

3. Бриндли К. Измерительные преобразователи: справочное пособие: пер. с англ. — М.: Энергоатомиздат, 1991. — 144 с.

4. Баскаков С.И. Радиотехнические цепи и сигналы: учеб. для вузов по спец. «Радиотехника». — 3-е изд., перераб. и доп. — М.: Высшая школа, 2000. — 462 с.: ил.

СВЕДЕНИЯ ОБ АВТОРАХ

Булгаков Олег Митрофанович. Заместитель начальника по учебной работе. Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: ombfrier@yandex.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473)2-735-290.

Стукалов Вадим Владиславович. Заместитель начальника кафедры. Кандидат технических наук.
Воронежский институт правительственной связи (филиал) Академии ФСО России.
E-mail: stvad@inbox.ru
Россия, 394042, г. Воронеж, ул. Минская, 2. Тел. 8-952-545-85-52.

Кучмасов Евгений Алексеевич. Специалист отделения конфиденциальной связи отдела организации конфиденциальной связи и криптозащиты интегрированной мультисервисной телекоммуникационной системы центра специальной связи.

ФКУ «Главный центр связи и защиты информации МВД России».
E-mail: ekuchmasov@mail.ru
Россия, 141407, Московская область, г. Химки, Юбилейный проспект, 59в. Тел. (495) 667-60-81.

Bulgakov Oleg Mitrofanovich. The deputy head on study. Doctor of technical sciences, professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473)2-735-290.

Stukalov Vadim Vladislavovich. The deputy chief of chair. Candidate of technical sciences.
Voronezh Institute of Government Communications (branch) of Academy of the Federal Protective Service of the Russian Federation.
Work address: Russia, 394042, Voronezh, Minskaya Str., 2. Tel. 8-952-545-85-52.

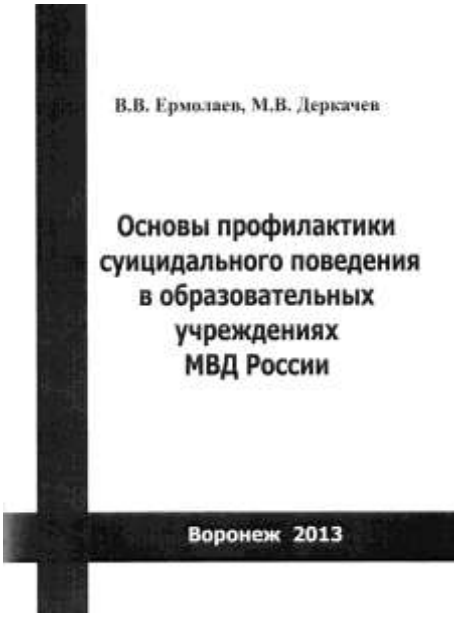
Kuchmasov Evgeniy Alekseevich. The expert of confidential communication section of confidential communication organization and cryptographic protection of information department of special communication unit.
The Main Center of Communication and Cryptographic Protection of Information of the Ministry of the Interior of Russia.
Work address: Russia, 141407, Moscow region, Khimki, Ubileynyi Prospect, 59в. Tel. (495) 667-60-81.

Ключевые слова: модель надежности; система защиты информации; объект информатизации; декомпозиция; вероятность отказа; последовательно-параллельная схема.

Key words: reliability model; information protection system; object information; decomposition; probability of failure; serial-parallel scheme.

УДК 654.01

ИЗДАНИЯ ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ



Ермолаев В.В.
Основы профилактики суицидального поведения в образовательных учреждениях МВД России: методическое пособие / В.В. Ермолаев, М.В. Деркачев. — 2-е изд., перераб. и доп. — Воронеж: Воронежский институт МВД России, 2013. — 88 с.
Методическое пособие разработано на основе материалов отечественных и зарубежных исследований суицидального поведения, современных подходов к профилактике самоубийств и предназначено для руководителей подразделений, сотрудников кадровых аппаратов и подразделений морально-психологического обеспечения.

В.П. Ирхин,
доктор технических наук, доцент, Воронежский институт ФСИН России

А.Н. Лукин,
доктор технических наук, профессор, Воронежский институт ФСИН России

С.Н. Панычев,
доктор технических наук, доцент, Воронежский институт ФСИН России

СПОСОБ ПОВЫШЕНИЯ АДАПТИВНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ К НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ И ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ

METHOD OF INCREASE OF THE ADAPTIVE INFORMATION-CONTROL SYSTEMS OF CRITICAL APPLICATION TO TAMPERING AND EMERGENCIES

Предложен новый способ распознавания несанкционированных воздействий при наличии жестких ограничений на временной и вычислительный ресурс подсистемы защиты информационно-управляющей системы критического применения и произведена его оценка. Показано, что он повышает адаптивность защитных механизмов информационно-управляющей системы, что снижает риск возникновения чрезвычайной ситуации.

A new method for detection of unauthorized actions in the presence of severe restrictions on the time and computational resource protection subsystem management information systems of critical applications and its assessment are made. It is shown that it increases the adaptability of the protective mechanisms of information management system, which reduces the risk of an emergency.

Распознавание, как известно, является одной из ключевых проблем выявления несанкционированных воздействий на информационно-управляющие системы критического применения (ИУС КП), особенно остро стоящей в условиях ограничения временного и вычислительного ресурса на работу подсистемы защиты информации (ПСЗИ). Также необходимо отметить, что задача распознавания информационного воздействия сводится к решению трех подзадач: сбор первичной информации; ее предварительная обработка с целью формирования совокупности признаков (нормировка, от-

бор, сопоставление и т.д.) и классификация, т.е. принятие решения о том, к какому из заданных классов относится наблюдаемое воздействие [1].

Рассмотрим более конкретно задачу классификации. Эффективность выполнения данной задачи в конкретных условиях напрямую зависит от выбранного метода классификации. Все известные методы, использующие понятие расстояния, предполагают наличие одного или нескольких эталонов для каждого класса.

Задача распознавания может быть сформулирована следующим образом. Имеется множество взаимоисключающих классов $\Omega = (\Omega_1,..., \Omega_m)$, каждый класс состоит из объектов, принадлежность объектов классу определяется соответствующей ему совокупностью признаков, причем количество признаков для всех классов фиксировано. Рассматривается некоторый объект ω, представленный в виде результатов наблюдений (измерений) его признаков. Задача распознавания состоит в том, чтобы отнести исследуемый объект ω к одному из взаимоисключающих классов Ω_i, где $i = \overline{1,m}$.

Условиями выполнения этой задачи является применение системы выявления вредоносных воздействий на ИУС КП, используемую при интенсивном информационном противодействии, как следствие, ограниченность времени для принятия решения о контрпротиводействии. Таким образом, способ распознавания вредоносных воздействий должен обеспечивать эффективное функционирование ИУС КП в динамично меняющихся условиях. Рассмотрим известные методы распознавания. Существует метод распознавания, основанный на использовании алгоритма минимума расстояния [2—4]. В данном методе используется словарь признаков (таблица).

Словарь признаков

Классы	Объекты	Значения признаков			
		X_1	X_2	…	X_N
Ω_1	ω_{11}	$x_{11,1}$	$x_{11,2}$	…	$x_{11,N}$
	ω_{12}	$x_{12,1}$	$x_{12,2}$	…	$x_{12,N}$
	…	…	…	…	…
	ω_{1r}	$x_{1r,1}$	$x_{1r,2}$	…	$x_{1r,N}$
…	…	…	…	…	…
Ω_m	ω_{m1}	$x_{m1,1}$	$x_{m1,2}$	…	$x_{m1,N}$
	ω_{m2}	$x_{m2,1}$	$x_{m2,2}$	…	$x_{m2,N}$
	…	…	…	…	…
	ω_{mr}	$x_{mr,1}$	$x_{mr,2}$	…	$x_{mr,N}$

В нем на языке этих признаков описаны объекты $\omega_{ij} = (X_{ij1}, X_{ij2},..., X_{ijN})$, где $i = \overline{1,m}$, $j = \overline{1,r}$, которые составляют классы распознавания Ω_i, где $i = \overline{1,m}$. При появлении в информационном N-мерном пространстве I воздействия $\omega = (x_1, x_2,..., x_N)$, не совпадающего по характеристикам ни с одним объектом ни одного из известных классов воздействий, вычисляют среднеквадратичное расстояние L_i, где $i = \overline{1,m}$, между распозна-

ваемым объектом и классом путем перебора и усреднения расстояний d_{ij}^2, где $i=\overline{1,m}$, $j=\overline{1,r}$, между неизвестным объектом и объектами, составляющими класс (рис. 1).

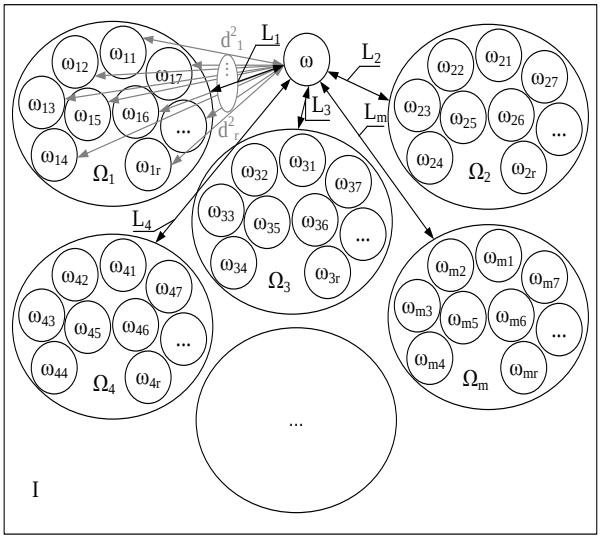


Рис. 1. Определение меры близости с использованием алгоритма минимума расстояний

Для этого по формуле (1) рассчитывают расстояние между объектами

$$d^2{}_{ij}=\sum_{p=1}^{N}(x_{\omega_{ij}}^{(p)}-x_{\omega}^{(p)})^2, \qquad (1)$$

где $i=\overline{1,m}$, $j=\overline{1,r}$.

Далее вычисляют среднеквадратичное расстояние $L(\omega,\Omega_i)$ между распознаваемым объектом и классом по формуле

$$L(\omega,\Omega_i)=\sqrt{\frac{1}{r_i}\sum_{j=1}^{r_i}d^2(\omega,\omega_{ij})}, \qquad (2)$$

где $i=\overline{1,m}$, $j=\overline{1,r}$.

Подобную процедуру повторяют для каждого класса. На основании близости к какому-либо классу принимают решение о принадлежности рассматриваемого объекта ω к этому классу Ω_i, где $i=\overline{1,m}$. Решающее правило выглядит следующим образом:

$$\omega\in\Omega_i, \text{ если } L_i(\omega,\Omega_i)=\min\{L_i(\omega,\Omega_i)\}. \qquad (3)$$

Данный метод обладает следующими недостатками: большие вычислительные затраты при увеличении количества объектов рассматриваемых классов и анализируемых признаков и, как следствие, большое количество времени при принятии решения.

Еще одним методом распознавания является метод, основанный на использовании алгоритма «ближайших соседей» [1]. Сущность этого метода похожа на метод, основанный на использовании алгоритма минимума расстояний, однако принадлежность неизвестного объекта ω классу Ω_i, где $i=\overline{1,m}$, определяется вычислением меры близости для класса не усреднением расстояний d_{ij}^2, где $i=\overline{1,m}$, $j=\overline{1,r}$, а определением

наибольшего количества из K объектов принадлежащих одному классу и находящихся на минимальном от него расстоянии. Решающее правило выглядит следующим образом:

$$\omega \in \Omega_i, \text{ если } L = \max_i \sum_{b=1}^{K} \delta_{ib}, \quad (4)$$

где δ_{ib} — символ Кронекера, $\delta_{ib} = 1$ при $b \in i$, $i = \overline{1,m}$ и $\delta_{ib} = 0$ при $b \notin i$, $i = \overline{1,m}$, K — пороговое значение ближайших соседей.

Недостатками данного метода, как и предыдущего, являются большие вычислительные затраты при увеличении количества рассматриваемых объектов и анализируемых признаков, а также малая эффективность при осуществлении вредоносного воздействия.

Также существует предложенный Журавлевым Ю.И. метод, относящийся к многоэтапным методам распознавания и основанный на использовании алгоритма «вычисления оценок» (АВО) [2—4]. Сущность метода заключается в определении степени похожести распознаваемого объекта, в нашем случае вредоносного воздействия, на объекты, входящие в состав априорно известного класса по так называемым системам опорных множеств.

Опыт решения задач распознавания свидетельствует о том, что часто основная информация заключена не в отдельных признаках, а в их сочетаниях. Поскольку не всегда известно, какие именно сочетания информативны, то в методе АВО степень похожести объектов вычисляется не последовательным сопоставлением отдельных признаков, а сопоставлением всех возможных (или определенных) сочетаний признаков, входящих в описание объектов. Совокупность признаков принятых в качестве информативных в каждом конкретном случае составляет систему опорных множеств Γ_t, где t изменяется от 1 до максимально принятого значения опорных множеств.

В общем случае реализация метода АВО сводится к формализации следующих этапов:

1) выделяется система опорных множеств Γ_t, по которым производится анализ распознаваемых объектов;

2) вводится понятие близости на множестве частей описаний объектов;

3) задаются правила.

Решающее правило в данном методе может принимать различные формы, в частности распознаваемая строка признаков может быть отнесена к классу, которому соответствует максимальная оценка меры близости, например

$$\omega \in \Omega_i \Leftrightarrow \max_i Y_{\Gamma_t}(\omega, \Omega_i), \quad (5)$$

где $i = \overline{1,m}$, $t = \overline{1,t_{\max}}$, $Y_{\Gamma_t}(\omega, \Omega_i)$ — мера близости на множестве частей описаний объектов, определяемая по формуле

$$Y_{\Gamma_t}(\omega, \Omega_i) = \sum_{t=1}^{t_{\max}} \Gamma_t(\omega, \Omega_i), \quad (6)$$

либо эта оценка будет превышать оценки всех остальных классов не меньше чем на определенную пороговую величину λ и т.д.

Однако этот метод при определенном достоинстве, таком как простота исполнения, все же обладает недостатком, это значительное число машинных операций при большой мощности словаря признаков, что снова неприемлемо в условиях ограничения временного и вычислительного ресурса.

Таким образом, рассмотренные методы неэффективны в условиях быстроменяющейся информационной обстановки.

Решим эту проблему следующим образом. Пусть, как в предыдущих случаях, существует словарь признаков (таблица), в котором на языке этих признаков описаны объекты, составляющие классы распознавания. Причем условием распознавания является то, что ошибка измерения меры близости неопознанного объекта к классу не должна превышать величины $R(\Omega_{i-1}, \Omega_i)$ — меру близости между классами, определяемую по формуле

$$R(\Omega_{i-1}, \Omega_i) = \sqrt{\frac{1}{r_{i-1} r_i} \sum_{v=1}^{r_{i-1}} \sum_{t=1}^{r_i} d^2(\omega_{i-1v}, \omega_{it})}, \qquad (7)$$

где $i = \overline{1,m}$, $d^2(\omega_{m-1v}, \omega_{mt})$ — расстояния между объектами соседних классов;

r — количество объектов в классе.

Выделим дополнительно в словаре признаков границы класса распознавания, состоящие из объектов класса, которые описываются экстремальными (максимальными или минимальными) значениями по одному и более признакам.

Пример описания границ класса в двухмерном информационном пространстве показан на рис. 2.

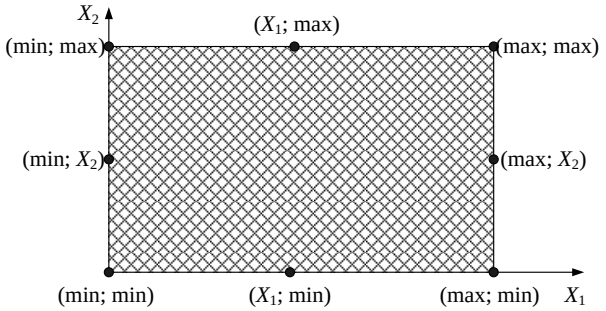


Рис. 2. Пример описания границ класса распознавания в двухмерном информационном пространстве

При появлении неопознанного вида воздействий в информационном N-мерном пространстве I, меру близости L_i, где $i = \overline{1,m}$, определяем путем вычисления расстояния до границы класса (рис. 3).

Для этого по формуле (1) вычисляем расстояние d^2_{irp1}, где $i = \overline{1,m}$, от объекта распознавания ω до граничного объекта ω_{irpmin}, где $i = \overline{1,m}$ с координатами, имеющими минимальные значения для данного класса распознавания Ω_i, где $i = \overline{1,m}$. Далее вычисляем расстояние d^2_{irp2}, где $i = \overline{1,m}$, от объекта распознавания ω до граничного объекта ω_{irpmax}, где $i = \overline{1,m}$ с координатами, имеющими максимальные значения для данного класса распознавания Ω_i, где $i = \overline{1,m}$.

Сравниваем полученные расстояния d^2_{irp1} и d^2_{irp2}, где $i = \overline{1,m}$. В случае если $d^2_{\text{irp1}} < d^2_{\text{irp2}}$, то вычисляем $d^2{}_{\text{irp2}+k_z}$ расстояния, где $i = \overline{1,m}$, $k_z = \overline{1, C_N^{s_q}}$, значение $C_N^{s_q}$ находим по формуле

$$C_N^{s_q} = \frac{N!}{(N-s_q)!s_q!}. \quad (8)$$

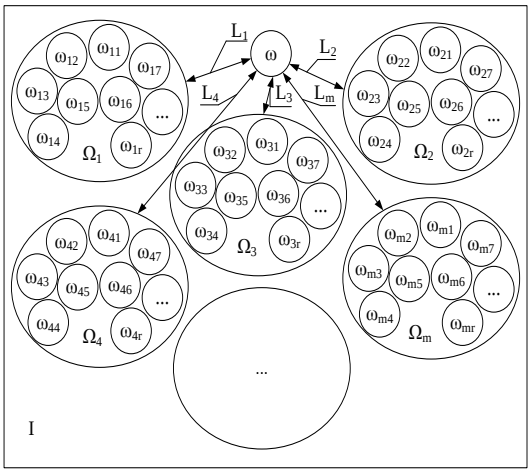


Рис. 3. Определение меры близости до границы класса

Значения величин $d^2_{\text{iгр2}+k_z}$ — это расстояния до граничных объектов $\omega_{\text{iгр}*}$, где $i=\overline{1,m}$ с координатами, имеющими $s_q=1$ значений максимальными, остальные — минимальными для данного класса распознавания Ω_i, где $i=\overline{1,m}$. Сравниваем полученные расстояния и определяем минимальное из них.

После этого вычисляем расстояния $d^2_{\text{iгр2}+k}$, где $i=\overline{1,m}$, k, находим по формуле

$$k=\left(\sum_{g=1}^{y} C_N^g\right)+k_{z+y}, \quad (9)$$

где $k_{z+y}=\overline{1,C_N^{s_{q+y}}}$, $C_N^{s_{q+y}}$ находим согласно выражению (8), в котором $s_{q+y}=s_q+y$, $y=\overline{1,(N-2)}$.

Полученные величины — это расстояния до граничных объектов $\omega_{\text{iгр}*}$, где $i=\overline{1,m}$, с координатами, имеющими $s_{q+y}=s_q+y$, где $y=\overline{1,(N-2)}$ значений — максимальные, остальные — минимальные для данного класса распознавания Ω_i, где $i=\overline{1,m}$. Сравниваем полученные расстояния и определяем минимальное из них.

В случае если $d^2_{\text{iгр1}} > d^2_{\text{iгр2}}$, где $i=\overline{1,m}$, вычисляем расстояния $d^2_{\text{iгр2}+k_z}$, где $i=\overline{1,m}$, $k_z=\overline{1,C_N^{s_q}}$, значение $C_N^{s_q}$ определяем по формуле (8).

Полученные значения величин являются расстояниями до граничных объектов $\omega_{\text{iгр}*}$, где $i=\overline{1,m}$ с координатами, имеющими $s_q=1$ значений минимальными, остальные — максимальными для данного класса распознавания Ω_i, где $i=\overline{1,m}$. Сравниваем полученные расстояния и определяем минимальное из них.

Далее вычисляем расстояния $d^2_{\text{iгр2}+k}$, где $i=\overline{1,m}$, k находим по формуле (9).

Полученные величины — это расстояния до граничных объектов $\omega_{i\text{гр}^*}$, где $i=\overline{1,m}$ с координатами, имеющими $s_{q+y}=s_q+y$, где $y=\overline{1,(N-2)}$ минимальные, остальные максимальные для данного класса распознавания Ω_i, где $i=\overline{1,m}$. Сравниваем полученные расстояния и определяем минимальное из них.

В результате полученных вычислений получаем *N* расстояний от объекта распознавания ω до граничных объектов класса $\omega_{i\text{гр}^*}$, где $i=\overline{1,m}$, все эти объекты имеют одну общую координату x_p, где $p=\overline{1,N}$, и отличаются друг от друга также по одной координате x_{p^*}, где $p=\overline{1,N}$. Запоминаем значение общей координаты.

Далее рассматриваем пару граничных объектов, отличающихся друг от друга только по одной координате x_{p^*}, где $p=\overline{1,N}$, находим значение этой координаты для ближайшего объекта, принадлежащего классу распознавания по формуле

$$x_{p^*}=\frac{d^2_{i\,\text{гр}}(..,x_{p\min},..)+a^2-d^2_{i\,\text{гр}}(..,x_{p\max},..)}{2\cdot a^2}+x_{p\min}, \qquad (10)$$

где $a=(x_{p\max}-x_{p\min})$ — расстояние между объектами, принадлежащими классу распознавания и отличающимися только по одной координате, $d^2_{i\,\text{гр}}(..,x_{p\min},..)$ и $d^2_{i\,\text{гр}}(..,x_{p\max},..)$ — расстояние от объекта распознавания ω до граничных объектов класса $\omega_{i\text{гр}^*}$, где $i=\overline{1,m}$, отличающихся только по одной координате и имеющих минимальное $x_{p\min}$ и максимальное $x_{p\max}$, где $p=\overline{1,N}$ — значение этой координаты соответственно.

Данную процедуру повторяем для всех пар граничных объектов, отличающихся друг от друга только по одной координате.

Таким образом, мы получим координаты граничного объекта $\omega_{i\text{гр}^*}$, где $i=\overline{1,m}$, находящегося на наименьшем удалении от объекта распознавания ω. Вычислим расстояние $d^2_{i\text{гр}^*}$, где $i=\overline{1,m}$, от объекта распознавания ω до найденного граничного объекта $\omega_{i\text{гр}^*}$, где ω — найденное значение $d^2_{i\text{гр}^*}$, где $i=\overline{1,m}$, является искомой величиной L_i, где $i=\overline{1,m}$.

Далее на основании близости $L=\min\{L_i\}$, где $i=\overline{1,m}$, к какому-либо классу принимается решение о принадлежности рассматриваемого объекта ω, вредоносного воздействия, к этому классу Ω_i, где $i=\overline{1,m}$.

Решающее правило выглядит так же, как в методе, основанном на использовании алгоритма минимума расстояния (формула (3)).

Однако преимущества, в отличие от вышеизложенных методов, очевидны. Во-первых, уменьшается количество машинных операций для определения принадлежности неизвестного объекта к определенному классу, так как предложенный способ не зависит от количества объектов, составляющих класс. На рис. 4 зависимости 1 и 2 соответствуют применению классического метода распознавания при Ω_i=6, ω_j=300 и ω_j=1000 соответственно, где $i=\overline{1,m}$, $j=\overline{1,r}$. Зависимость 3 соответствует применению предлагаемого способа распознавания при Ω_i=6 и ω_j=1000, где $i=\overline{1,m}$, $j=\overline{1,r}$.

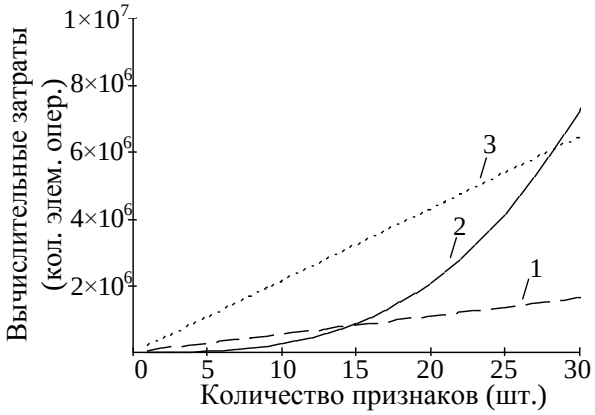


Рис. 4. График зависимости вычислительных затрат от количества объектов и признаков распознавания

Во-вторых, при неизменной мощности словаря признаков время на распознавания значительно сокращается, так как, в отличие от остальных методов, в предложенном способе рассматриваются лишь объекты, находящиеся на границе класса, и совершенно не учитываются объекты, принадлежащие классу, но находящиеся глубже по параметрам признакового пространства.

Таким образом, анализируя все достоинства предложенного способа, можем сказать, что с его применением появляется возможность использовать высвободившийся ресурс (временной и вычислительный) для увеличения количества анализируемых параметров несанкционированных воздействий, а это, в свою очередь, увеличивает адаптивность защитных механизмов ИУС КП, что снижает риск возникновения чрезвычайной ситуации.

ЛИТЕРАТУРА

1. Душкин А.В. Методическое обеспечение системы выявления несанкционированных воздействий на информационные телекоммуникационные системы специального назначения в условиях ограничения временного ресурса: монография. — Воронеж: ВАИУ, 2010. — 192 с.

2. Горелик А.Л., Скрипкин В.А. Методы распознавания: учеб. пособие для вузов. — М.: Высшая школа, 1977. — 222 с.

3. Миленький А.В. Классификация сигналов в условиях неопределенности. Статистические методы самообучения в распознавании образов. — М.: Советское радио, 1975. — 328 с.

4. Фукунага К. Введение в статистическую теорию распознавания образов. — М.: Наука, 1979. — 368 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Ирхин Валерий Петрович. Профессор кафедры основ радиотехники и электроники. Доктор технических наук, доцент.
Воронежский институт ФСИН России.
E-mail: a_dushkin@mail.ru
Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. (473) 260-68-19.

Лукин Александр Николаевич. Заместитель начальника по научной работе. Доктор технических наук, профессор.
Воронежский институт ФСИН России.
E-mail: a_dushkin@mail.ru
Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. (473) 260-68-19.

Панычев Сергей Николаевич. Профессор кафедры технических комплексов охраны и связи. Доктор технических наук, доцент.
Воронежский институт ФСИН России.
E-mail: a_dushkin@mail.ru.
Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. (473) 260-68-19.

Irkhin Valeriy Petrovich. Professor of foundations of radio and electronics. Doctor of technical sciences, assistant professor.
Voronezh Institute of the Russian Federal Penitentionary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 260-68-19.

Lukin Alexander Nikolaevich. Deputy chief of Voronezh Institute of the Russian Federal Penitentionary Service for research. Doctor of technical sciences, professor.
Voronezh Institute of the Russian Federal Penitentionary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 260-68-19.

Panychev Sergey Nikolaevich. Professor of technical systems of protection and communication. Doctor of technical sciences, assistant professor.
Voronezh Institute of the Russian Federal Penitentionary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 260-68-19.

Ключевые слова: класс; признак; объект; метод; расстояние; мера близости; граница; информационное пространство.

Key words: class; identifier; object; method; distance; nearness measure; boundary; information space.

УДК 004.9

В.В. Меньших,
доктор физико-математических наук, профессор

А.Ф. Самороковский,
кандидат технических наук

А.В. Корчагин

МОДЕЛЬ ДЕЙСТВИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ ТЕХНОГЕННОГО ХАРАКТЕРА

MODEL OF ACTIONS OF LAW-ENFORCEMENT BODIES IN THE EMERGENCY SITUATIONS OF TECHNOGENIC CHARACTER

Разработаны математические модели развития чрезвычайных ситуаций техногенного характера и действий органов внутренних дел, а также установлена взаимосвязь между этими моделями.

Mathematical models of development of emergency situations of technogenic character and actions of police department are developed, and also the interrelation between these models is established.

Введение. На территории Российской Федерации сохраняется довольно высокий уровень угрозы чрезвычайных ситуаций (ЧС) техногенного характера. Наибольшую опасность представляют аварии в системах критического применения, к которым относятся системы, существенно влияющие на жизнеобеспечение большого количества граждан, экологию значительных территорий или экономическое развитие целых регионов: атомные и электростанции, крупные предприятия, транспортная система и т.п.

Возникновение чрезвычайных ситуаций техногенного характера обусловлено физическим износом основных производственных фондов, нарушениями установленных норм и правил эксплуатации опасных объектов, снижением требовательности и персональной ответственности должностных лиц за эти нарушения [1]. Примерами могут служить следующие ЧС [2]:

аварии на транспортных коммуникациях (пожару на газопроводе в Москве 2009 года была присвоена наивысшая пятая категория сложности);

аварии на АЭС с разрушением производственных сооружений и радиоактивным заражением территории (авария на Чернобыльской АЭС);

гидродинамические аварии — прорыв плотин, дамб (авария на Саяно-Шушенской ГЭС).

Основными задачами органов внутренних дел (ОВД) при ликвидации ЧС техногенного характера являются охрана общественного порядка и участие в спасательных работах, что должно обеспечивать защиту населения и территории от чрезвычайных ситуаций, минимизировать риски и опасности. Тот факт, что в последнее время наблюдается тенденция роста количества и масштабов последствий чрезвычайных ситуаций [3], а также структурные изменения, происходящие в системе МВД и, в том числе, в подразделениях охраны общественного порядка, участвующих в ликвидации ЧС, заставляют искать новые пути решения проблемы управления ОВД, оптимизации процессов принятия управленческих решений. Решение этой задачи возможно на основе использования специально разработанных математических моделей, чему посвящен целый ряд публикаций. Однако в этих моделях либо не учитывались особенности ЧС техногенного характера [4, 5], либо решались частные задачи [6].

В настоящей работе разрабатывается математическая модель для выбора сотрудниками ОВД оптимальных действий по ликвидации последствий ЧС, а также в процессе обучения принятию управленческих решений.

Действия органов внутренних дел при возникновении ЧС техногенного характера. В зависимости от развития ЧС могут использоваться различные алгоритмы действий сотрудников ОВД и пути решения поставленных задач. Расчеты сил и средств производятся с целью создания оптимальной группировки, необходимой для выполнения задач по ликвидации ЧС.

Органы внутренних дел при введении чрезвычайного положения, в случае возникновения ЧС техногенного характера, привлекаются для выполнения следующих основных задач [7]:

-поддержание особого режима въезда на территорию, на которой введено чрезвычайное положение, и выезда с нее;

-охрана объектов, обеспечивающих жизнедеятельность населения и функционирование транспорта, и объектов, представляющих повышенную опасность для жизни и здоровья людей, а также для окружающей природной среды;

- участие в ликвидации чрезвычайных ситуаций и спасении жизни людей в составе сил Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций.

Помимо выполнения своих основных функций в ОВД при необходимости могут создаваться группы тушения пожаров, проведения неотложных аварийно-спасательных работ, медицинского, тылового (материально-технического), технического обеспечения, взаимодействия со средствами массовой информации [8].

Мероприятия по ликвидации последствий чрезвычайных ситуаций техногенного характера, к выполнению которых привлекаются силы и средства органов внутренних дел, определяются республиканской (краевой и областной) комиссией по чрезвычайным ситуациям. Этой же комиссией дается часть исходных данных для расчета сил и средств (общий характер и размер возможных чрезвычайных ситуаций), а также гидрометеорологический, сейсмотектонический, медико-бактериологический и ветеринарно-бактериологический прогнозы [8].

Управление действиями ОВД в таких сложных ситуациях требует незамедлительного и правильного принятия решений от руководителей. Силами ОВД при ликвидации

последствий ЧС техногенного характера для выполнения задач организуется система оперативного управления в составе оперативного штаба и функциональных групп (ФГ) [6].

Руководство оперативным штабом при ликвидации последствий ЧС техногенного характера осуществляется в форме организации действий функциональных групп. В действиях оперативного штаба различают четыре этапа работы [8]:

первый этап — распределение функциональных обязанностей между членами штаба, сбор информации и оценка ситуации;

второй этап — подготовка сил и средств к действиям при ЧС и выбор тактики действий;

третий этап — реализация тактики действий путём оперативного управления силами и средствами в ходе ликвидации аварии, материально-технического обеспечения, медицинской помощи, всесторонней оперативной связи и взаимодействия, осуществления контроля между ФГ, корректировки действий сил, а также для решения основных задач;

четвёртый этап — свёртывание сил и возвращение района заражения к нормальной жизнедеятельности.

Развитие событий существенно зависит от условий, масштаба, характера чрезвычайной ситуации, последствия которой трудно предвидеть. Процесс выполнения задач, решаемых сотрудниками ОВД, существенно зависит от характера самой ЧС [8].

Решая задачи по ликвидации ЧС техногенного характера и их последствий, органы внутренних дел проводят различные мероприятия, применяют разнообразные способы, приемы, методы, но все это они делают не стихийно, а планомерно, в определенной последовательности, с учетом конкретной ситуации.

Мероприятия, в том числе и подготовительные, которые проводятся в ОВД, являются одной из форм ликвидации чрезвычайных ситуаций. Решения, принимаемые оперативным штабом, должны быть не произвольными, а целенаправленными, учитывающими возможные изменения обстоятельств.

Поэтому для более детального изучения и дальнейшего моделирования действий сотрудников ОВД при ЧС техногенного характера необходимо разработать модель развития самой ЧС.

Моделирование чрезвычайных ситуаций техногенного характера. Несмотря на разнообразие вариантов развития для каждого типа ЧС всегда можно выделить отдельные стадии развития ЧС и условия перехода от одной стадии к другой. Как правило, в ЧС техногенного характера выделяют следующие стадии [1,2]:

ω_0 — стадия отсутствия ЧС;

ω_1 — стадия накопления отклонений от нормального состояния или процесса (стадия зарождения ЧС);

ω_2 — наличие события, лежащего в основе ЧС;

ω_3 — стадия особо опасного развития событий, во время которой происходит высвобождение источника опасности (энергии или вещества), приводящая к риску неблагоприятного воздействия на население, объекты и природную среду;

ω_4 — стадия затухания, которая хронологически охватывает период от перекрытия (ограничения) источника опасности, т.е локализации чрезвычайной ситуации, до полной ликвидации её прямых последствий, проведение профилактических мероприятий.

Условия перехода от стадии к стадии описаны в табл. 1.

Таблица 1

Описание переходов между стадиями ЧС

Переход между стадиями	Обозначение	Условие возникновения событий, приводящих к переходу от стадии к стадии
$\omega_0 - \omega_0$	x_0	Отсутствие ЧС
$\omega_0 - \omega_1$	x_1	Нарушение технологического процесса, сбои подачи ресурсов, сложность технологий и т.п.
$\omega_1 - \omega_0$	x_2	Переход объекта ЧС в режим нормального функционирования в результате профилактических мероприятий, планово-предупредительных работ ГУ МЧС России на потенциально опасных и критически важных объектах.
$\omega_0 - \omega_2$	x_3	Возникновение события в результате резкого изменения внутренних или внешних причин (недостаточная квалификация и некомпетентность обслуживающего персонала, проектно-конструкторские недоработки в механизмах и оборудовании, терроризм, войны, стихийные бедствия и т.п.).
$\omega_1 - \omega_2$	x_4	Накопление факторов риска до критического значения и возникновения событий, лежащих в основе ЧС.
$\omega_1 - \omega_1$	x_5	Процесс постоянного воздействия опасных факторов.
$\omega_2 - \omega_3$	x_6	Высвобождение источника опасности.
$\omega_2 - \omega_1$,	x_7	Ликвидация событий, которые могли привести к ЧС.
$\omega_2 - \omega_2$	x_8	Наличие неустраненных чрезвычайных событий, которые могут привести к ЧС.
$\omega_3 - \omega_2$	x_9	Прекращение воздействия источника опасности.
$\omega_3 - \omega_3$	x_{10}	Неустраненный процесс высвобождения источника опасности (энергии или вещества).
$\omega_3 - \omega_4$	x_{11}	Устранение процесса высвобождения источников опасности.
$\omega_4 - \omega_4$	x_{12}	Постоянное действие остаточных факторов и сложившихся чрезвычайных условий.
$\omega_4 - \omega_0$	x_{13}	Переход объекта ЧС в режим нормального функционирования.
$\omega_2 - \omega_0$	x_{14}	Полная ликвидация событий, которые могли привести к ЧС.
$\omega_0 - \omega_3$	x_{15}	Резкое высвобождение источников опасности.

Полученное описание позволяет представить математическую модель ЧС техногенного характера в виде конечного автомата Мура [9] $A = (\Omega, X, \lambda)$ с алфавитом состояний $\Omega = \{\omega_0, \ldots, \omega_4\}$, алфавитом входов $X = \{x_1, \ldots, x_{15}\}$, функции переходов λ. Ав-

томат является неполным, т. к. переходы между некоторыми стадиями неосуществимы. Графически автомат *A* может быть представлен в виде диаграммы Мура (рис.1).

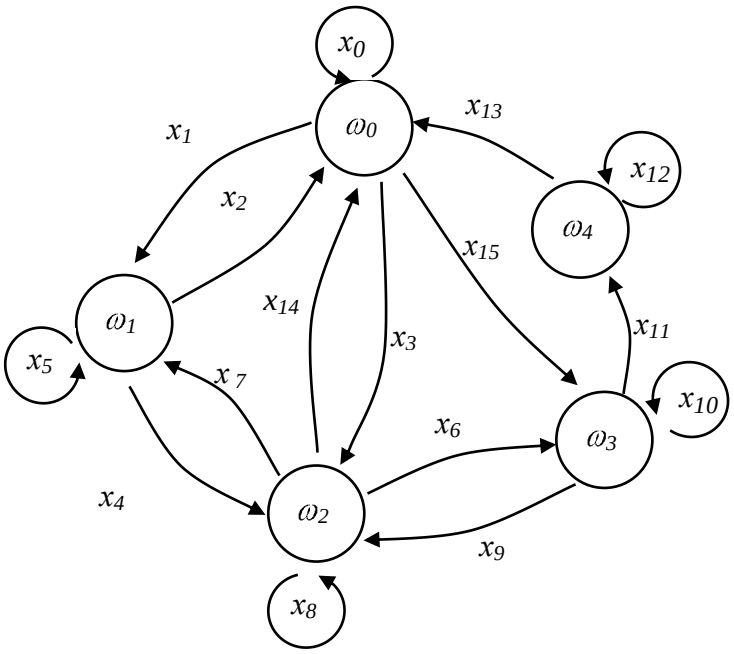


Рис. 1. Диаграмма Мура автоматной модели развития ЧС техногенного характера

Модель действий органов внутренних дел в динамике ЧС техногенного характера. В процессе развития ЧС техногенного характера ОВД осуществляют следующие действия:

s_0 — Режим повседневной деятельности ОВД.

s_1 — Уточнение информации, сбор, обобщение и анализ данных о возможном ЧС, первоначальная оценка ситуации.

s_2 — Первоначальные распоряжения, предварительные указания ФГ

s_3 — Выработка решений, выбор тактики действий ФГ, определяется структура системы управления действиями, формирование сил и средств, постановка задач и управление ФГ, определение порядка взаимодействия с другими силами.

s_4 — Решение ФГ поставленных задач.

s_5 — Завершение действий ОВД, подведение итогов, прекращение работы ФГ

Условия перехода от выполнения одного действия к другому представлены в табл. 2.

Полученное описание позволяет представить математическую модель действий органов внутренних дел в динамике ЧС техногенного характера также в виде конечного автомата Мура $B = (S, Y, \mu)$ с алфавитом состояний $S = \{s_0, \ldots, s_5\}$, алфавитом входов $Y = \{y_1, \ldots, y_9\}$, функцией переходов μ.

Автомат *B* также является неполным и графически может быть представлен в виде диаграммы Мура (рис. 2).

Таблица 2

Описание переходов между этапами работы ОШ

Переход	Обозначение	Условие перехода
$s_0 - s_0$	y_0	Отсутствие ЧС.
$s_0 - s_1$	y_1	Поступление сигнала о чрезвычайном событии, который может привести к ЧС техногенного характера.
$s_1 - s_0$	y_2	Ликвидация событий на первоначальном этапе.
$s_1 - s_1$	y_3	Изменение хода и масштабов ЧС, продолжительности времени сбора информации.
$s_1 - s_2$	y_4	Выполнение необходимых действий ФГ на первоначальном этапе проведения мероприятий по ликвидации ЧС.
$s_2 - s_3$	y_5	Обстоятельства, определяющие дальнейшие действия ФГ (Данные о силах и средствах, обработка первоочередной информации на основе данных о ЧС).
$s_3 - s_4$	y_6	Команда на выполнение поставленных задач.
$s_4 – s_5$	y_7	Успешное завершение действий ФГ по выполнению поставленных задач.
$s_4 – s_3$	y_8	Корректирование тактики действий сотрудников ОВД, в связи с изменением хода и масштаба ЧС.
$s_5 – s_0$	y_9	Переход ОВД в режим повседневной деятельности.

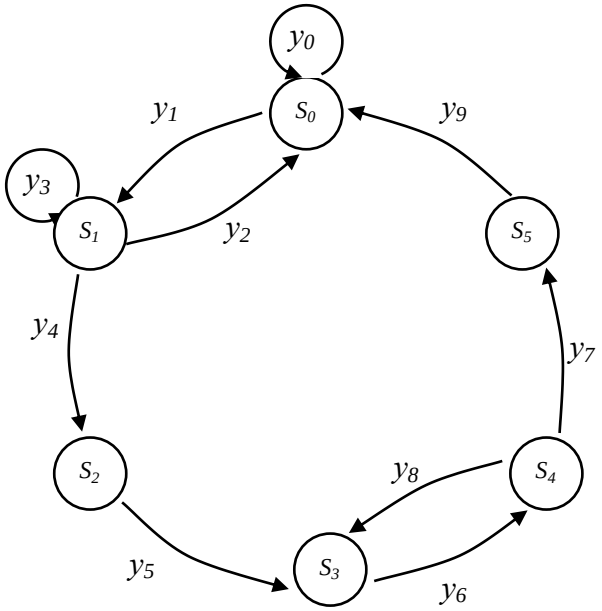


Рис. 2. Диаграмма Мура автоматной модели действий ОВД при ЧС техногенного характера

Автоматы *A* и *B* являются взаимосвязанными: смена состояний в автоматной модели B определяется сменой состояний в автоматной модели *A*. Например, переход из состояния s_1 в состояние s_2 в автомате B происходит, если в автомате *A* осуществлён переход из состояния ω_2 в состояние ω_3. Переход в автомат B инициируется переходом в автомат *A*.

Полный перечень связей между автоматами представлен в табл. 3.

Таблица 3

№ п/п	Переход в автомате *B*	Переход в автомате *A*, который приводит к переходу в автомате *B*
1	y_0	x_0
2	y_1	x_3, x_4
3	y_2	x_2, x_{13}
4	y_3	x_6, x_8, x_{14}
5	y_4	x_6, x_8, x_{14}
6	y_5	x_9
7	y_6	$x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{14}$
8	y_7	x_{13}
9	y_8	$x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{14}$
10	y_9	x_0

Таким образом, следует рассматривать сеть [9], состоящую из двух автоматов *A* и *B*, что может быть использовано для разработки имитационной модели действий ОВД. Различные подходы использования сетей автоматов содержится в [5, 10].

Заключение. Разработанные взаимосвязанные автоматные модели развития чрезвычайных ситуаций техногенного характера и действий ОВД в процессе развития этих ЧС могут быть детализированы за счёт описаний работы отдельных функциональных групп и оперативного штаба, что позволит осуществлять оценку эффективности действий ОВД.

ЛИТЕРАТУРА

1. Федоров А.Ю. Организация деятельности ОВД при авариях и катастрофах технологического характера: монография. — 2009. — С. 155—170.

2. Гафнер В.В., Петров С.В., Забара Л.И. Опасности социального характера и защита от них: учеб. пособие. — М.: Флинта: Наука, 2012. — 320 с.

3. Постановление Правительства РФ от 07.07.2011 № 555. О федеральной целевой программе «Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в Российской Федерации до 2015 года».

4. Меньших В.В., Пьянков О.В., Самороковский А.Ф. Выбор оптимального варианта действий органов внутренних дел при чрезвычайных обстоятельствах на основе экстраполяции экспертных оценок // Вестник Воронежского государственного технического университета. — 2008. — Том 4. — № 3. — С. 166—168.

5. Меньших В.В., Лунев Ю.С., Самороковский А.Ф. Алгоритм имитационного моделирования действий органов управления и подразделений органов внутренних дел

при возникновении чрезвычайных обстоятельств // Вестник Воронежского института МВД России. — 2007. — № 2. — С. 125—129.

6. Меньших В.В., Самороковский А.Ф., Корчагин А.В. Математические методы и информационно-технические средства: Труды VIII Всероссийской научно-практической конференции, 22—23 июня 2012 г. — Краснодар: Краснодарский университет МВД России, 2012. — С 141—144.

7. Федеральный Конституционный закон Российской Федерации от 30 мая 2001 года № 3-ФКЗ «О чрезвычайном положении».

8. Бондаревский И.И. Специальная тактика: учебник. — М.: ЦОКР МВД России, 2005. — 368 с.

9. Кудрявцев В.Б., Алешин С.В., Подколозин А.С. Введение в теорию автоматов — М.: Наука, 1985. — 320 с.

10. Сысоев В.В., Меньших В.В., Солодуха Р.А., Забияко С.В. Исследование взаимодействий в сети конечных детерминированных автоматов // Радиотехника. — 2000. — № 9. — С. 65—67.

СВЕДЕНИЯ ОБ АВТОРАХ

Меньших Валерий Владимирович. Начальник кафедры высшей математики. Доктор физико-математических наук, профессор.

Воронежский институт МВД России.

E-mail: menshikh@list.ru

Россия, 394065, проспект Патриотов, 53. Тел. (473) 262-33-79.

Самороковский Андрей Федорович. Начальник кафедры тактико-специальной подготовки. Кандидат технических наук.

Воронежский институт МВД России.

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. 8-905-656-16-34.

Корчагин Андрей Викторович. Преподаватель кафедры тактико-специальной подготовки.

Воронежский институт МВД России.

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. 8-910-340-10-18.

Menshikh Valery Vladimirovich. The chief of the chair of High Mathematics. Doctor of physical and mathematical sciences, professor.

Voronezh Instinute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 262-33-79.

Samorokovskiy Andrey Fedorovich. The chief of tactics and special training chair.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8-905-656-16-34.

Korchagin Andrey Viktorovich. Lecturer of tactics and special training chair.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8-910-340-10-18.

Ключевые слова: чрезвычайные ситуации техногенного характера; действия органов внутренних дел; математическая модель.

Key words: emergency situations of technogenic character; action of police department; mathematical model.

УДК 519.876.2:351.74

Д. В. Волков,
Управление вневедомственной охраны Главного управления МВД России по Свердловской области

А.В. Мельников,
кандидат технических наук

В.В. Навоев,
кандидат технических наук, Управление вневедомственной охраны Главного управления МВД России по Свердловской области

ТЕХНИКО-ЭКОНОМИЧЕСКАЯ ЭКСПЕРТИЗА ОБЪЕМНЫХ ИЗВЕЩАТЕЛЕЙ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ

TECHNICAL AND ECONOMIC EXAMINATION OF THE VOLUME DETECTORS OF THE SECURITY AND FIRE ALARM SYSTEM

Предложена методика экспертизы современных приборов охранно-пожарной сигнализации (объемных извещателей), основанная на использовании метода анализа иерархий. Рассмотрены детерминированный и нечетко-множественный показатели качества и сравниваются между собой полученные результаты.

The technique of examination of modern devices of the security and fire alarm system (volume detectors), based on use of a method of the analysis of hierarchies is offered. The determined and indistinct and multiple indicators of quality are considered and among themselves received results are compared.

Для практической деятельности подразделений вневедомственной охраны весьма важной задачей является рациональный выбор технических средств из имеющегося в распоряжении перечня. При этом очень важно выбрать средство не только наилучшее по своим техническим характеристикам, но и удовлетворяющее заданным ограничениям по стоимости. Таким образом, речь идет о комплексном технико-экономическом обследовании доступных на рынке приборов. Научно обоснованный подход к решению этой задачи заключается в использовании методов экспертизы.

В работе [1] приводится методика экспертизы приемно-контрольных приборов охранно-пожарной сигнализации, продемонстрировавшая свою эффективность. Более развернутое описание этой методики приведено в работе [2]. В частности, анализируется специфика применения к задачам экспертного оценивания идей известного аналити-

ка Т. Саати [3, 4] и предложена модификация метода анализа иерархий, а также охарактеризовано применение понятий и методов теории нечетких множеств.

Целью данной статьи является технико-экономическая экспертиза другого класса приборов вневедомственной охраны — объемных извещателей, использующих различные физические принципы (радиолокация, ультразвук, пиротехнический эффект). Между собой сравниваются три модели извещателей, представленных на современном рынке («Астра-551», «Сокол-2», «Орлан»).

Проведем далее сравнительную экспертизу объемных извещателей охранно-пожарной сигнализации, основные характеристики которых приведены в табл. 1.

Таблица 1

Основные характеристики современных объемных извещателей

№	Наименование	«Астра-551»	«Сокол-2»	«Орлан»
Количественные характеристики				
1	Длина минимальной зоны обнаружения, м	10	12	6
2	Ширина минимальной зоны обнаружения, м	6	6	5
3	Контролируемая минимальная скорость детекции, м/с	0,3	0,3	0,35
4	Токопотребление в дежурном режиме, мА	16	20	35
Наличие (отсутствие) определенных свойств				
5	Наличие регистрации вскрытия извещателя	Нет	Да	Да
6	Наличие радиоканала (эффект Доплера)	Эффект Доплера (радиоканал), пироэлектрический эффект	Эффект Доплера (радиоканал), пироэлектрический эффект	Регистрация акустических колебаний, пироэлектрический эффект
7	Наличие радиоволновой или инфракрасной зоны обнаружения извещателя (РВ-эллипс), (ИК-объем)	РВ-эллипс, ИК-объем	РВ-эллипс, ИК-объем	АК (акустический) объем
Качественные характеристики				
8	Помехозащищенность (наличие дополнительных каналов связи, специализированных алгоритмов и процессоров распознавания помех)	Средняя (микроконтроллер извещателя, выдает сигнал лишь при одновременном поступлении сигналов с 2 датчиков	Средняя (микроконтроллер извещателя, выдает сигнал лишь при одновременном поступлении сигналов с 2 датчиков)	Высокая (микропроцессорная обработка сигнала, режим самотестирования, срабатывание лишь по 2 каналам связи)

9	Эргономичность для клиента (удобство пользования для собственника — наличие внешних индикаторов, возможности установки без прокладки проводов)	Низкая (наличие индикатора срабатывания извещателя, передача сигналов о срабатывании возможна только по проводам)	Низкая (наличие индикатора срабатывания извещателя, передача сигналов о срабатывании возможна только по проводам)	Средняя (наличие индикатора срабатывания, возможность раздельного функционирования охранных датчиков
10	Эстетичность (внешний вид, цветовая гамма, размеры, возможность скрытой установки)	Средняя (невозможность скрытой установки, компактное устройство, внешний вид современный , только белый)	Ниже средней (невозможность скрытой установки, габариты извещателя выше чем средние, внешний вид современный)	Средняя (невозможность скрытой установки, компактное устройство, внешний вид современный,)
Стоимостные характеристики				
11	Цена извещателя, руб.	1054	1348	1106

Выбор признаков объектов экспертизы. Первым этапом экспертизы объемных извещателей является анализ обычно применяемых показателей качества объектов и разделение их на подмножества количественных признаков, качественных признаков, признаков наличия, признаков психофизиологической природы и т.д. Введем признаки x_i, соответствующие приведенным в табл.1 характеристикам объемных извещателей.

Как видно (см. табл.1), первые четыре показателя являются количественными признаками $x_{j,кол}$, $j = 1-4$, причем первый и второй признаки являются признаками положительного эффекта (ППЭ), т.е. увеличение их значений должно привести к росту обобщенного показателя качества $J_{кач}$. Третий и четвертый признаки являются признаками отрицательного эффекта (ПОЭ), т.е. их увеличение приведет к уменьшению обобщенного показателя качества $J_{кач}$. Такой характер признаков потребует в дальнейшем применения к ним различной нормировки.

Пятый — седьмой показатели являются признаками наличия, соответственно, x_5—x_7. Восьмой — десятый показатели являются качественными признаками x_8—x_{10}, оцениваются группой экспертов по пятибалльной шкале и подвергаются статистической обработке.

Одиннадцатый показатель x_{11} является ценой объекта экспертизы P и также относится к признакам отрицательного эффекта.

Обобщенный показатель качества. Рассмотрим мультипликативную модель детерминированного комплексного показателя «качество — цена» [2]:

$$J = \left[\hat{V}_{кол} \frac{\sum_j V_{j,кол} x_{j,кол}}{\sum_j V_{j,кол}} + \hat{V}_{нал} \frac{\sum_i V_{i,нал} x_{i,нал}}{\sum_i V_{i,нал}} + \hat{V}_{кач.пр.} \frac{\sum_l V_{l,кач.пр.} \overset{\Delta}{x}_{l,кач.пр.}}{\sum_l V_{l,кач.пр.}} \right] \times$$

$$\times \frac{\hat{V}_{цены}\ \hat{P}}{\hat{V}_{кол}+\hat{V}_{нал}+\hat{V}_{кач.пр.}} = J_{\text{кач}} \cdot J_{\text{цены}}, \qquad (1)$$

где $\hat{V}_{кол}, \hat{V}_{нал}, \hat{V}_{кач.пр.}$ — нормированные групповые весовые коэффициенты, определяющие относительную предпочтительность количественных признаков, признаков наличия и качественных признаков, соответственно; множества V_j, V_i, V_l определяют векторы приоритетов, т.е. относительный вклад отдельных признаков (частных критериев); $\hat{P}_{цены}$ — нормированная функция цены. Приведем далее правила нормировки количественных, качественных признаков и признака цены, последовательно.

Признаки положительного эффекта. Количественные признаки определяются из прайс-листов, технических описаний и другой документации и усреднения по группе экспертов не требуют. Предполагается, что признаки наличия принимают значения 0 или 1, и для них нормировка не предусмотрена.

Качественные признаки оцениваются экспертами в баллах по пятибалльной шкале и усредняются по группе экспертов. Операция усреднения отражается верхней чертой над обозначением соответствующего признака в формуле (1).

Для того чтобы обеспечить однородный вклад различных слагаемых во взвешенную сумму (1), необходимо привести их значения к единому диапазону. Для этого введем следующую нормировку

$$x_j = \frac{x_j}{x_{j,баз}}, \quad j = 1,2,\ldots, m, \quad x_{j,баз} = \max_k x_j^{(k)}, \quad k = 1,2,\ldots,K \qquad (2)$$

Нормированные таким образом значения признаков принадлежат единичному интервалу $x_j \in [0,1], \forall j$. Применительно к процедуре пятибалльного оценивания можно принять $x_{j,баз} = 5$.

Признаки отрицательного эффекта. Для данной задачи экспертизы признаками отрицательного эффекта являются x_3, x_4 и x_{11}. В отличие от формулы (2), для них требуется иная нормировка:

$$\hat{x}_i = \frac{x_{i,баз}}{x_i}, \qquad x_{i,баз} = \min_k x_i^{(k)} \quad k = 1,2,\ldots . \qquad (3)$$

Цена объекта также является признаком отрицательного эффекта, и для ее нормировки используем разновидность формулы (3)

$$\hat{P}^{(k)} = \frac{P_{баз}}{P^{(k)}}, \qquad (4)$$

где $P_{баз}$ — минимальная цена по группе сравниваемых объектов, $P^{(k)}$ — цена k-го объекта экспертизы.

Приведем в единой таблице значения признаков x_i и их нормированные значения x_i (табл. 2).

Таблица 2

Нормированные значения признаков и функции принадлежности

Номер признака	«Астра-551»			«Сокол-2»			«Орлан»		
	x_i	$\hat{x}_i$	μ_i	x_i	$\hat{x}_i$	μ_i	x_i	$\hat{x}_i$	μ_i
Количественные признаки									
1	10	0,833	1,000	12	1,000	1,000	6	0,500	0,501
2	6	1,000	1,000	6	1,000	1,000	5	0,833	1,000
3	0,3	1,000	1,000	0,3	1,000	1,000	0,35	0,857	1,000
4	16	1,000	1,000	20	0,800	1,000	35	0,457	0,429
Сумма взвешенных признаков		0,929	0,929	—	0,976	0,976	—	0,651	0,514
Признаки наличия									
5	0	0,000	0,000	1	1,000	1,000	1	1,000	1,000
6	1	1,000	1,000	1	1,000	1,000	0	0,000	0,000
7	1	1,000	1,000	1	1,000	1,000	0	0,000	0,000
Сумма взвешенных признаков		0,460	0,460	—	1,000	1,000	—	0,539	0,539
Качественные признаки									
8	3,2	0,640	0,734	3,2	0,640	0,734	4,8	0,960	1,000
9	3,1	0,620	0,701	3,1	0,620	0,701	3,8	0,760	0.935
10	3,6	0,720	0,868	2,9	0,580	0,634	3,6	0,720	0,868
Сумма взвешенных признаков		0,646	0,482	—	0,628	0,450	—	0,887	0,865
Показатели качества $J_{кач}, J_{кач}$		0,807	0.769	—	0,899	0.858	—	0,691	0.597
Функция цены									
11	8000	0,562	0,604	7500	0,600	0,668	4500	1,000	1,000
Качество — цена J, J		0,453	0,260	—	0,539	0,344	—	0,691	0,597

Нечетко-множественный показатель качества. Нечетко-множественная мультипликативная модель комплексного показателя «качество — цена» согласно работе [2] имеет вид

$$J = \left[\hat{V}_{кол} \frac{\sum_j V_{j,кол} \mu_{A_{jj}} \hat{x}_j}{\sum_j V_{j,кол}} + \hat{V}_{нал} \frac{\sum_i V_{i,нал} \hat{x}_i}{\sum_i V_{i,нал}} + V_{кач.пр.} \frac{\sum_l V_{l,кач} \mu_{A_L} \hat{x}_l}{\sum_l V_{l,кач.пр.}} \right] \times \frac{\mu_P(\hat{P}) \hat{P}}{V_{кол} + V_{нал} + V_{кач}} = J_{кач} \cdot J_{цены}, \quad (5)$$

где μ_{A_j}, μ_{A_i}, μ_{A_l}, μ_P — функции принадлежности множествам допустимых значений количественных признаков, признаков наличия, качественных признаков и цены, соответственно.

Введенные выше нормировки признаков (2), (3) имеют большое методическое значение. При этом все нормированные признаки изменяются в диапазоне [0, 1], и для всех этих признаков может быть выбрана единая функция принадлежности. Для случая односторонней трапецеидальной функции ее форма задается характеристическим Т-множеством $T = t_1, t_2, t_3, t_4$.

Выберем в нашей задаче единую форму функции принадлежности μ с характеристическим множеством $T = 0{,}2; 0{,}8; 1{,}0; 1{,}0$. Рассчитанные значения μ_i для каждого из признаков приведены в табл.2 (третий столбец для каждого из сравниваемых приборов).

Векторы приоритетов признаков. Следующей задачей является оценка множеств $V_{кол}, V_{нал}, V_{кач.пр.}$, $V_{j,кол}$, $V_{i,нал}$, $V_{l,кач.пр.}$, т.е. векторов приоритетов. Воспользуемся методом анализа иерархий Т.Саати, согласно которому один из сравниваемых признаков выбирается в качестве основного (опорного), а остальные сравниваются с ним по степени уменьшения важности согласно лингвистической шкале [3,5]. Упомянутые степени снижения важности второстепенных признаков по сравнению с главным (опорным) часто называют рангами r_j. Отметим обратную зависимость: чем выше ранг, тем менее значим признак.

В основе метода анализа иерархий лежит построение матрицы парных сравнений W , определение собственных чисел и собственных векторов матрицы W из уравнения

$$AV = \lambda V, \tag{6}$$

где V — искомый вектор весовых коэффициентов. Максимальное собственное число λ_{max} служит для оценки согласованности матрицы W , а первый собственный вектор нормируется делением на сумму его элементов.

Проиллюстрируем методику определения вектора приоритетов на примере определения *групповых весовых коэффициентов*. Учитывая относительную важность отдельных групп признаков, составим матрицу парных сравнений

$$W_{груп} = \begin{bmatrix} 1 & 5 & 3 \\ 0{,}2 & 1 & 0{,}5 \\ 0{,}33 & 2 & 1 \end{bmatrix}. \tag{7}$$

При построении матрицы $W_{груп}$ было принято, что для объемных извещателей наиболее значимыми признаками являются количественные признаки (ранг равен 1), несколько менее значимыми — качественные признаки (ранг равен 3), наименее значимыми — признаки наличия (ранг равен 5).

Определим собственные числа матрицы $W_{груп}$ из уравнения (6). Расчеты показывают, что максимальное собственное число матрицы $\lambda_{max} = 3{,}001$. Индекс согласо-

ванности ИС = 0,00051, отношение согласованности ОС = 0,00086. Итак, сформированная матрица $W_{груп}$ оказалась хорошо согласованной.

Определим собственные векторы матрицы парных сравнений (7):

$$eigenvecs(W_{груп}) = \begin{bmatrix} 0{,}928 & 0{,}925 & 0{,}925 \\ 0{,}175 & -0{,}085-0{,}154i & -0{,}085+0{,}154i \\ 0{,}328 & -0{,}168+0{,}291i & -0{,}168-0{,}291i \end{bmatrix}. \quad (8)$$

Как видим, второй и третий собственные векторы оказались комплексно сопряженными. Причина этого состоит в инверсии рангов, входящих в первую строку матрицы парных сравнений (7). При расстановке рангов в порядке возрастания (1, 3, 5) второй и третий векторы оказываются вещественными, как показано в статье [1].

Разделив первый собственный вектор на сумму его элементов 1,431, получим нормированный вектор приоритетов различных групп признаков

$$V_{груп} = \begin{pmatrix} 0{,}649 & 0{,}122 & 0{,}229 \end{pmatrix}^T. \quad (9)$$

Учитывая относительную важность различных *количественных признаков* (см. табл.1), составим матрицу парных сравнений

$$W_{кол} = \begin{bmatrix} 1 & 2 & 2 & 3 \\ 0{,}5 & 1 & 1 & 2 \\ 0{,}5 & 1 & 1 & 2 \\ 0{,}33 & 0{,}5 & 0{,}5 & 1 \end{bmatrix}. \quad (10)$$

При построении матрицы $W_{кач}$ было принято, что наиболее значимым признаком является длина минимальной зоны обнаружения (ранг равен 1), несколько менее значимыми — ширина минимальной зоны обнаружения и контролируемая минимальная скорость детекции (ранги равны 2), менее значимым — токопотребление в дежурном режиме (ранг равен 3).

Определим собственные числа матрицы $W_{кол}$ из равенства (10). Расчеты показывают, что максимальное собственное число матрицы $\lambda_{max} = 4{,}007$. Индекс согласованности ИС = 0,0023, отношение согласованности ОС = 0,0026. Итак, сформированная матрица $W_{кол}$ оказалась достаточно хорошо согласованной.

Определим собственные векторы матрицы парных сравнений (10):

$$eigenvecs(W_{кол}) = \begin{bmatrix} 0{,}777 & 0{,}885 & 0{,}923 & 0{,}887 \\ 0{,}416 & -0{,}158+0{,}225i & -0{,}158-0{,}225i & 0{,}707 \\ 0{,}416 & -0{,}158+0{,}225i & -0{,}158-0{,}225i & -0{,}707 \\ 0{,}224 & -0{,}086-0{,}242i & -0{,}086+0{,}242i & 0{,}000 \end{bmatrix}.$$

Разделив первый собственный вектор на сумму его элементов 1,833, получим нормированный вектор приоритетов количественных признаков

$$V_{кол} = \begin{pmatrix} 0{,}424 & 0{,}227 & 0{,}227 & 0.122 \end{pmatrix}^T. \quad (11)$$

Учитывая относительную важность различных *признаков наличия* (см. табл.1), составим матрицу парных сравнений

$$W_{нал} = \begin{bmatrix} 1 & 2 & 3 \\ 0{,}5 & 1 & 2 \\ 0{,}33 & 0{,}5 & 1 \end{bmatrix}. \qquad (12)$$

При построении матрицы $W_{нал}$ было принято, что для объемных извещателей наиболее значимым признаком наличия является возможность регистрации вскрытия извещателя (ранг равен 1), несколько менее значимым — наличие радиоканала (ранг равен 2), менее значимым — наличие радиоволновой или инфракрасной зоны обнаружения (ранг равен 3).

Определим собственные числа матрицы $W_{нал}$ из уравнения (12). Расчеты показывают, что максимальное собственное число матрицы $\lambda_{max} = 3{,}006$. Индекс согласованности ИС = 0,0031, отношение согласованности ОС = 0,0051. Итак, сформированная матрица $W_{нал}$ оказалась хорошо согласованной.

Определим собственные векторы матрицы парных сравнений:

$$eigenvecs(W_{нал}) = \begin{bmatrix} 0{,}847 & 0{,}850 & 0{,}850 \\ 0{,}466 & -0{,}237 + 0{,}397i & -0{,}237 - 0{,}397i \\ 0{,}256 & -0{,}126 - 0{,}2181i & -0{,}126 + 0{,}218i \end{bmatrix}. \qquad (13)$$

Разделив первый собственный вектор на сумму его элементов 1,569, получим нормированный вектор приоритетов признаков наличия

$$\hat{V}_{нал} = (0{,}540 \quad 0{,}297 \quad 0{,}163)^T. \qquad (14)$$

Результаты расчетов суммы взвешенных признаков наличия также приведены в табл.2.

Учитывая относительную важность отдельных групп *качественных* признаков, составим матрицу парных сравнений

$$W_{кач} = \begin{bmatrix} 1 & 3 & 5 \\ 0{,}33 & 1 & 1{,}5 \\ 0{,}2 & 0{,}5 & 1 \end{bmatrix}. \qquad (15)$$

При построении матрицы $W_{кач}$ было принято, что наиболее значимым признаком является помехозащищенность (ранг равен 1), несколько менее значимым — эргономичность для клиента (ранг равен 3), наименее значимым — эстетичность (ранг равен 5).

Определим собственные числа матрицы $W_{кач}$ из равенства (6). Расчеты показывают, что максимальное собственное число матрицы $\lambda_{max} = 2{,}909$. Индекс согласованности ИС = 0,045, отношение согласованности ОС = 0,078. Итак, сформированная матрица $W_{кач}$ оказалась достаточно хорошо согласованной.

Определим собственные векторы матрицы парных сравнений (15):

$$eigenvecs(W_{кач}) = \begin{bmatrix} 0{,}937 & 0{,}984 & 0{,}344 \\ 0{,}301 & -0{,}128 & 0{,}777 \\ 0{,}177 & -0{,}128 & -0{,}526 \end{bmatrix}.$$

Разделив первый собственный вектор на сумму его элементов 1,415, получим нормированный вектор приоритетов различных качественных признаков

$$\hat{V}_{кач} = (0{,}662 \quad 0{,}213 \quad 0{,}125)^T. \qquad (16)$$

Как видим, применение методики кластерно-иерархического подхода [2] к экспертизе объемных извещателей привело к необходимости 4 раза применить метод анализа иерархий. Воспользовавшись найденными векторами приоритетов групповых признаков (9), количественных признаков (11), признаков наличия (14), качественных признаков (16), составим объединенную таблицу (табл.3).

Таблица 3

Векторы приоритетов различных групп признаков

Признаки	Ранги r_i	λ_{max}	ОС	Вектор приоритетов V
количественные	(1,2,2,3)	4,007	0,0026	0,424 0,227 0,227 0,122
наличия	(1,2.3)	3,006	0,0051	0,540 0,297 0,163
качественные	(1,3,5)	2,909	0,0782	0,662 0,213 0,125
групповые	(1,5,3)	3,001	0,0009	0,649 0,122 0,229

Воспользовавшись полученными выше оценками векторов приоритетов V, нормированными значениями признаков $\hat{x}_i$ и соответствующими значениями функций принадлежности $\mu_i(\hat{x}_i)$ (см. табл. 2), найдем взвешенные суммы каждой из этих групп признаков. Результаты расчетов приведены в соответствующих строках табл. 2.

Это позволяет, с учетом вектора приоритета групповых признаков (9), найти детерминированный и нечетко-множественный показатели качества $J_{кач}, \tilde{J}_{кач}$. Как видим, среди сравниваемых объемных извещателей наилучшие показатели качества имеет «Сокол-2» ($J_{кач}$=0,899), а наихудшие — «Орлан» ($J_{кач}$=0,691).

После определения функции цены окончательно определим комплексные показатели «качество-цена» $J, \tilde{J}$ (см. последнюю строку табл. 2). В результате сравнения объемных извещателей с учетом цены ситуация изменилась: наиболее предпочтительным является «Орлан» (J=0,691), а на втором месте — «Сокол-2» (J=0,539). Извещатель «Астра-551» оказался наименее привлекательным изделием по соотношению качества и цены (J=0,453).

Предлагаемая методика позволяет эффективно проводить экспертизу сложных технических объектов, характеристики которых зависят от множества факторов (признаков) с учетом стоимостных ограничений. Как было показано выше, нечетко-множественный показатель качества оказывается более чувствительным к различию свойств сравниваемых приборов.

В целом, применение принципа разделения признаков и четырехкратное использование метода анализа иерархий позволяет значительно повысить объективность экспертизы, поскольку даже администратор экспертного эксперимента до последнего момента не знает, какой объект получит наибольшую рейтинговую оценку.

ЛИТЕРАТУРА

1. Бухарин С.В., Мельников А.В., Навоев В.В. Экспертиза приемно-контрольных приборов охранно-пожарной сигнализации // Вестник Воронежского института МВД России. — 2013. — №1. — С. 123—130.

2. Бухарин С.В., Мельников А.В. Кластерно-иерархические методы экспертизы экономических объектов: монография. — Воронеж: Научная книга, 2012. — 276 с.

3. Саати Т. Принятие решений: Метод анализа иерархий: пер. с англ. — М.: Радио и связь, 1993. — 278 с.

4. Саати Т.Л. Принятие решений при зависимостях и обратных связях. Аналитические сети: пер. с англ. — М.: Издательство ЛКИ, 2008. — 360 с.

5. Дилигенский Н.В., Дымова Л.Г., Севастьянов П.В. Нечеткое моделирование и многокритериальная оптимизация производственных систем в условиях неопределенности: технология, экономика, экология. — М.: Машиностроение-1, 2004. — 397 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Волков Дмитрий Александрович. Заместитель начальника отдела Управления вневедомственной охраны Главного управления МВД России по Свердловской области.

Управление вневедомственной охраны Главного управления МВД России по Свердловской области.

E-mail: volfmvd@rambler.ru

Россия, 620142, г. Екатеринбург, ул. Чапаева, 12а. Тел. (343) 257-62-50.

Мельников Александр Владимирович. Старший преподаватель кафедры огневой подготовки. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: meln78@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2623-397.

Навоев Виктор Владимирович. Начальник Управления вневедомственной охраны Главного управления МВД России по Свердловской области. Кандидат технических наук.

Управление вневедомственной охраны Главного управления МВД России по Свердловской области.

E-mail: v.navoev@ mail.ru

Россия, 620142, г. Екатеринбург, ул. Чапаева, 12а. Тел. (343) 257-62-50.

Volkov Dmitry Alexandrovich. The deputy chief of division of Department of Management of private security of Central administrative board of the Ministry of the Interior of Russia on Sverdlovsk area.

Work address: Russia, 620142, Ekaterinburg, Chapaev Str., 12a. Tel. (343) 257-62-50.

Melnikov Alexander Vladimirovich. Senior lecturer of the chair of Range practice. Candidate of technical sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2623-397.

Navoev Victor Vladimirovich. The head of Department of private security of Central administrative board of the Ministry of the Interior of Russia on Sverdlovsk area. Candidate of technical sciences.

Work address: Russia, 620142, Ekaterinburg, Chapaev Str., 12a. Tel. (343) 257-62-50.

Ключевые слова: согласованность оценок экспертов; методы функционального анализа; деятельность подразделений полиции вневедомственной охраны.

Key words: coordination of estimations of experts; methods of the functional analysis; activity of divisions police of private security.

УДК 004.891

А.В. Паринов,
кандидат технических наук, доцент, Воронежский институт ФСИН России

С.В. Белокуров,
доктор технических наук, доцент, Воронежский институт ФСИН России

Д.Г. Зыбин,
кандидат технических наук, доцент, Воронежский институт ФСИН России

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ПРИМЕНЕНИЯ СТАТИСТИЧЕСКИХ ПОКАЗАТЕЛЕЙ И ВЕРОЯТНОСТНЫХ КРИТЕРИЕВ

ASSESSMENT OF THREATS TO THE SECURITY OF CONFIDENTIAL INFORMATION THROUGH THE USE OF STATISTICS AND PROBABILITY CRITERIA

Рассматривается актуальная научная проблема создания научно-методологических основ безопасности конфиденциальной информации с учетом воздействия на информационно-телекоммуникационные системы угроз различного характера.

The article deals with the problem of creating an actual scientific research and methodological foundations of security of confidential information, given the impact on the telecommunication system threats of various kinds.

Проблема, связанная с обеспечением безопасности конфиденциальной информации (КИ) от воздействия на информационно-телекоммуникационную систему (ИТКС) внешних и внутренних угроз в настоящее время приобретает особую актуальность. Указанная проблема подтверждается анализом имеющейся статистической информации о влиянии угроз на безопасность КИ, циркулирующей в ИТКС. Утечка КИ, интеллектуальной собственности, информации «ноу-хау» является следствием значительного материального и морального ущерба, который наносится собственнику информации ограниченного распространения.

Сложность и комплексность проблемы анализа и синтеза информационно-телекоммуникационных систем, иерархичность построения, присущая таким системам, предполагает, что оценка безопасности конфиденциальной информации должна осуществляться с применением системы показателей и критериев. Результаты такой оценки являются основой для принятия решений из некоторого множества альтернатив. Ис-

следования показывают, что в указанных целях наиболее перспективным является применение статистических показателей и вероятностных критериев.

Статистические показатели могут быть абсолютными и относительными. В то же время абсолютные и относительные статистические показатели подразделяются на общие и частные.

Общие показатели характеризуют безопасность КИ по всем факторам или причинам, приводящим к угрозам, а частные — по конкретным факторам и причинам или по группам причин.

К общим абсолютным статистическим показателям безопасности КИ можно отнести следующие [1]:

- общее число угроз, воздействующих на ИТКС за определенный период (сутки, месяц, год и т. п.) n_y;

- абсолютный ущерб, нанесенный собственнику в результате воздействия на ИТКС внутренних угроз (например, тыс. рублей) $R_{ущ}$.

Абсолютные статистические показатели могут применяться для:

- выявления общих тенденций в динамике угроз, воздействующих на ИТКС;

- выявления и прогноза общего ущерба от воздействия угроз на ИТКС;

- разработки и применения плановых профилактических мероприятий по предупреждению появления угроз, их локализации и снижения величины ущерба от их реализации.

Основным недостатком абсолютных статистических показателей является то, что они характеризуют уровень безопасности КИ за прошедший период и не позволяют осуществлять прогноз на ближайшую перспективу.

К общим относительным статистическим показателям безопасности КИ относятся [1]:

- средняя наработка ИТКС на одну внутреннюю угрозу за определенный период (например, за год)

$$T_{ср} = \frac{t_У}{n_y},$$

где $t_У$ — суммарная наработка ИТКС за определенный период; n_y — количество внутренних угроз, проявившихся за этот же период;

- средняя наработка ИТКС на одну внутреннюю угрозу с последствиями за определенный период (например, за год)

$$T_{ср} = \frac{t_У}{(n_y)_{пос}},$$

где $(n_y)_{пос}$ — количество угроз с последствиями за определенный период;

- средняя величина ущерба на одну угрозу с последствиями

$$\overline{R} = \frac{R_У}{(n_y)_{пос}},$$

где $R_У$ — суммарная величина ущерба собственнику за определенный период (например, за год).

Общие относительные показатели безопасности КИ позволяют оценить общую тенденцию изменения наработки и наработки с последствиями с учетом воздействия на ИТКС внутренних угроз. При этом следует отметить, что вследствие применения замкнутых механизмов, совершенствования политики безопасности, проведения органи-

зационно-профилактических мероприятий, данные показатели имеют устойчивую тенденцию повышения.

В целом общие статистические показатели имеют интегральный характер и не позволяют осуществить оценку и прогнозирование по отдельным угрозам, особенно тем, которые приводят к существенным последствиям. Эту задачу можно решить с помощью частных статистических показателей.

К частным статистическим показателям относятся [1]:

- распределение внутренних угроз по причинам, вызвавшим их появление (халатность, безответственность и т. п. сотрудников организации);
- распределение внутренних угроз по последствиям от воздействия на ИТКС (например, кража, подмена, уничтожение КИ и т. п.);
- распределение внутренних угроз по частоте появления однотипных внутренних угроз (например, частота кражи, подмены, перехвата КИ и т. п.);
- распределение внутренних угроз по степени риска собственнику КИ (например, наибольший, повышенный, средний, ограниченный, низкий и т. п.);
- распределение внутренних угроз по последствиям от воздействия внутренних угроз на КИ (например, катастрофические, критические, существенные, малосущественные, несущественные последствия).

Использование частных статистических показателей позволяет определить уровень безопасности КИ по отдельным внутренним угрозам, причинам, их вызвавшим, последствиям воздействия на ИТКС в целом и ее элементы. Использование информации, полученной в процессе принятия частных статистических показателей для анализа состояния безопасности КИ, предполагает разработку и проведение научно обоснованных мероприятий по предупреждению или полной ликвидации наиболее опасных внутренних угроз за счет проведения целевой профилактической работы среди сотрудников, допущенных к работе с КИ и пользователей КИ. Однако статистические показатели обладают существенными недостатками. Они заключаются в следующем [8]:

- такие показатели оценивают безопасность КИ за прошедший период;
- по таким показателям не представляется возможным осуществлять прогнозирование безопасности КИ.

Указанные недостатки можно парировать за счет принятия для оценки безопасности КИ вероятностных критериев.

Воздействие внутренних угроз на элементы системы ИТКС в общем виде носит случайный характер и может привести к двум исходам [2]:

- благополучный исход в случае, если цель воздействия внутренних угроз на ИТКС не достигнута;
- неблагополучный исход во всех остальных случаях.

В связи с этим в качестве критерия оценки безопасности КИ можно принять вероятность благополучного исхода при воздействии на ИТКС внутренних угроз [3].

Обозначим указанную вероятность через p. Вероятность противоположного события, т. е. вероятность неблагополучного исхода при воздействии на ИТКС внутренних угроз, будет равна q. Указанные события составляют полную группу независимых событий. Тогда

$$p + q = 1.$$

Нетрудно заметить, что вероятности p и q являются аналитическими критериями оценки безопасности КИ.

Как уже было отмечено, на безопасность КИ оказывают влияние многочисленные факторы [3]. Поэтому для оценки безопасности КИ могут применяться различные подходы. Однако, как показывает анализ [3], для такой оценки необходимо

учитывать тот факт, что в результате воздействия на ИТКС внутренних угроз она может перейти из исходного (нормального) состояния в другое, особое, состояние, соответствующее возникновению особой ситуации. В то же время появление особых ситуаций связано с угрозой безопасности КИ, циркулирующей в ИТКС.

Переход ИТКС из одного состояния в другое является следствием вполне конкретных причин. Однако возникают они, как правило, в произвольный момент времени, поэтому их появление случайно. Каждая особая ситуация может привести как к благополучному, так и неблагополучному исходу для КИ с учетом успешности (неуспешности) действий сотрудников по парированию последствий появления особых ситуаций.

Обозначим вероятность возникновения i-й особой ситуации через q_i, условную вероятность парирования ее последствий — через r_i, а вероятность непарирования — через $\overline{r_i}$.

Тогда для определения вероятностей p_i и q_i представим последовательность переходов ИТКС от одного (исходного) состояния к другому марковским случайным процессом со счетным множеством состояний и непрерывным временем. Такое представление обусловлено следующими допущениями:

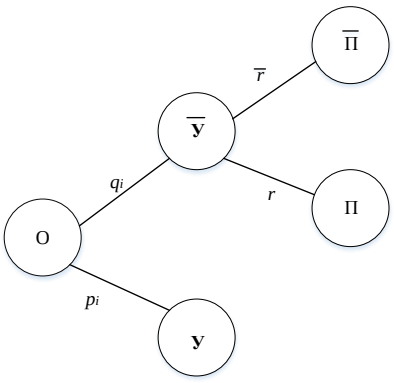
- в исходном состоянии ИТКС находится в нормальном состоянии;
- последовательность возникновения особых ситуаций i-го вида является простейшим потоком с интенсивностью λ_i;
- интенсивность благополучного исхода обозначена через $\lambda_i r_i$, а неблагополучного — через $\lambda_i \overline{r_i}$;

Сущность метода расчета вероятностей p_i и q_i при использовании марковского процесса состоит в том, что неизвестные вероятности определяются из решения дифференциальных уравнений, которые описывают этот процесс. Анализ показывает, что такой процесс целесообразно представить в виде логико-вероятностного процесса [3].

Предположим, что возможные состояния ИТКС в процессе воздействия на нее угроз определены. Кроме того, известны направления ее случайных переходов из состояния в состояние. Тогда вполне возможно построить логическую схему (граф) состояния , которая при известных вероятностях перехода системы из состояния в состояние представляет собой логико-вероятностную модель ИТКС (см. рисунок, по аналогии с [3]).

На рисунке представлена логическая схема воздействия на ИТКС одной i-й угрозы.

Правомочность такого представления ИТКС основана на том, что возможные исходы от воздействия на ИТКС являются случайными событиями в силу случайности появления тех или иных внутренних угроз.



Логико-вероятностный процесс воздействия на ИТКС i-й внутренней угрозы

В соответствии с рисунком следует, что в процессе функционирования ИТКС существует некоторая опасность, связанная с воздействием на нее i-й угрозы. При таком воздействии ИТКС может находиться в следующих состояниях (рис. 1):

- О — начальное состояние ИТКС;
- $У$ — состояние, когда i-я внутренняя угроза не проявляется с вероятностью p_i;
- $\overline{У}$ — состояние, когда i-я внутренняя угроза проявилась с вероятностью $q_i = 1 - p_i$;
- $П$ — состояние парирования внутренней угрозы с вероятностью r;
- $\overline{П}$ — состояние непарирования последствий проявления внутренней угрозы с вероятностью $\bar{r} = 1\text{-}r$.

Конечные состояния $\overline{У}$ и П соответствуют благополучному исходу при воздействии на ИТКС i-й угрозы.

Состояние $\overline{П}$ соответствует неблагополучному исходу при воздействии на ИТКС i-й внутренней угрозы. Тогда, в соответствии с рисунком вероятность благополучного исхода от воздействия на ИТКС i-й угрозы определяется следующим образом:

$$P_{бu_i} = p_i + q_i * r_i,$$

а вероятность неблагополучного исхода

$$Q_{бu_i} = q_i * \overline{r_i}.$$

Так как вероятности $P_{бu_i}$ и $Q_{бu_i}$ составляют полную группу событий, то:

$$P_{бu_i} + Q_{бu_i} = 1. \qquad (1)$$

Из (1) следует, что

$$P_{бu_i} = 1 - Q_{бu_i},$$

$$Q_{бu_i} = 1 - P_{бu_i}.$$

Таким образом, с точки зрения последствий воздействия на ИТКС внутренней угрозы на основе анализа выражения (1) можно сделать следующие выводы.

1. Количественной мерой, характеризующей последствия от воздействия i-й внутренней угрозы на КИ, являются вероятность благополучного исхода $P_{бu_i}$ и вероятность противоположного события, т. е. вероятность неблагополучного исхода в результате воздействия i-й внутренней угрозы на ИТКС, т. е. $Q_{бu_i}$.

2. Анализ выражения (1) свидетельствует о том, что вероятности $P_{бu_i}$ и $Q_{бu_i}$ являются критериями количественной оценки последствий от воздействия на ИТКС i-й внутренней угрозы.

3. Анализ выражения (1) также показывает, что для количественной оценки последствий воздействия внутренних угроз на ИТКС достаточно определить любую составляющую, например $Q_{бu_i}$. Определение другой составляющей из выражения (1) не представляет сложностей.

Таким образом, приведенная структура показателей и критериев свидетельствует о том, что наиболее перспективными являются аналитические критерии. Однако их применение для оценки уровня безопасности КИ затруднительно из-за отсутствия соответствующих математических моделей. Сложность проблемы заключается в том, что традиционные существующие математические модели не всегда приемлемы для ука-

занных целей. Следовательно, необходима разработка математических моделей, предназначенных для оценки безопасности КИ с учетом воздействия на ИТКС угроз.

ЛИТЕРАТУРА

1. Девянин П.Н. Модели безопасности компьютерных систем: учеб. пособие для студ. высш. учеб. заведений. — М.: Академия, 2005. —144 с.

2. Додонов А.П., Горбаник Е.С., Кузнецова М.П. Живучесть компьютерных систем и безопасность информационной инфраструктур // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». — 2007. — № 1(76). — С. 203—208.

3. Спиркин Г.Н., Юшков Е.С., Харьков С.А. Концептуальные направления защиты КИ // Информационная безопасность: сборник трудов научно-практической конференции. — Таганрог : Таганрог. радиотехн. ун-т, 2002. — С. 263—266.

СВЕДЕНИЯ ОБ АВТОРАХ

Паринов Андрей Владимирович. Профессор кафедры технических комплексов охраны и связи. Кандидат технических наук, доцент.
Воронежский институт ФСИН России.
E-mail: stimpson79@mail.ru
Россия, 394072, г. Воронеж, ул. Иркутская 1а. Тел. (473) 2606-818.

Белокуров Сергей Владимирович. Профессор кафедры управления и информационно-технического обеспечения. Доктор технических наук, доцент.
Воронежский институт ФСИН России.
E-mail: bsvlabs@comch.ru
Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. (473) 2606-819.

Зыбин Дмитрий Георгиевич. Начальник кафедры технических комплексов охраны и связи. Кандидат технических наук, доцент.
Воронежский институт ФСИН России.
E-mail: zdg77@mail.ru
Россия, 394072, г. Воронеж, ул. Иркутская 1а. Тел. (473) 2606-818.

Parinov Andrey Vladimirovich. Professor of the chair of technical systems of protection and communication. Doctor of technical sciences, assistant professor.
Voronezh Institute of the Russian Federal Penitentiary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 2606-818.

Belokurov Sergey Vladimirovich. Professor of the chair of Management and Information Technology Services. Doctor of technical science., assistant professor.
Voronezh Institute of the Russian Federal Penitentiary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 2606-819.

Zybin Dmitriy Georgievich. Head of the chair of technical systems of protection and communication. Candidate of technical sciences, assistant professor.
Voronezh Institute of the Russian Federal Penitentiary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a. Tel. (473) 2606-818.

Ключевые слова: конфиденциальная информация; угрозы; информационная безопасность; оценка уязвимостей.

Key words: confidential information, threats, information security, vulnerability assessment.

УДК 004.056.5

И.Г. Дровникова,
доктор технических наук, доцент

Д.А. Кабанов,
В/Ч 28683

К ВОПРОСУ УПРАВЛЕНИЯ КОНТРОЛЕМ ЦЕЛОСТНОСТИ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

TO THE QUESTION OF MANAGEMENT OF INTEGRITY CONTROL OF THE SPECIAL SOFTWARE OF THE AUTOMATED SYSTEM

Рассмотрена проблема управления контролем целостности рабочей среды автоматизированной системы (АС), являющаяся одной из базовых проблем организационно-технологического управления процессами защиты информации (ЗИ) в АС на основе применения программных средств защиты.

The problem of management by control of integrity of a working environment of the automated system, being one of basic problems of organizational and technological management of information security processes in the automated system on the basis of application of software of protection, is considered.

В настоящее время в АС на первый план выходят задачи обеспечения информационной безопасности (ИБ) [1], при этом, как показал опыт эксплуатации данных систем, наибольший вклад в нарушение ИБ АС вносят факты несанкционированного доступа (НСД) к информации [2]. Для решения задачи обеспечения ИБ в различных АС создаются системы защиты информации (СЗИ). СЗИ — совокупность органов и (или) исполнителей, используемой ими техники ЗИ, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области ЗИ [3].

Традиционно управление процессами защиты информации от НСД в АС имеет организационный характер, под которым следует понимать приказы, инструкции и т.д. организации, эксплуатирующей АС. В то же время этот вид управления имеет ряд существенных недостатков, которые значительно снижают защищённость АС [4]:

1. Низкий уровень автоматизации процессов управления подсистемами систем ЗИ (СЗИ) АС (практически все вышеуказанные функции возложены на администратора безопасности АС).

2. Открытыми остаются следующие вопросы:

управление длиной пароля СЗИ АС;

управление целесообразностью временной последовательности запуска главной тестовой программы контроля целостности специального программного обеспечения (СПО) АС (традиционно её запуск осуществляет администратор безопасности АС по собственной инициативе, при этом время запуска могут спрогнозировать как злоумышленник, так и пользователи АС);

управление временной последовательностью планирования использования специальных преобразований отдельных файлов АС.

3. Усиление функций ЗИ в СЗИ приводит к увеличению процессорного времени, что в целом негативно сказывается на решении задач АС по её прямому назначению.

В настоящее время в результате развития процесса математизации знания в широком спектре естественных, технических и общественных наук появилась возможность поставить на серьёзную математико-кибернетическую основу процесс принятия решений при управлении сложными системами и тем самым осуществить переход от существующего организационного управления к более перспективному организационно-технологическому управлению процессами ЗИ в АС на основе применения средств ЗИ.

Под организационно-технологическим управлением процессами ЗИ в АС на основе средств ЗИ следует понимать меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей АС, а также механизмы управления, реализуемые на базе программных средств управления процессами ЗИ в АС, позволяющие как программно поддерживать принятие управленческих решений, так и осуществлять их автоматическое принятие [1].

Так как проблема ЗИ от НСД является частью общей проблемы ИБ, то для ЗИ от НСД в АС создаётся в рамках соответствующей СЗИ система защиты информации от несанкционированного доступа — комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от НСД к информации в АС [5]. В соответствии с [6], СЗИ НСД в АС представляет собой функциональную подсистему АС, организованную как совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в АС для решения в ней необходимых задач ЗИ от НСД.

Несмотря на то что в действующих Руководящих документах Гостехкомиссии непосредственно не отражены вопросы управления ИБ, с помощью этих документов, тем не менее, можно выявить структуру задач управления процессами ЗИ в АС на основе программных средств защиты информации (ПСрЗИ), представленную на рисунке.

Согласно [7] обеспечение защиты АС осуществляется системой разграничения доступа (СРД) субъектов к объектам доступа и обеспечивающими средствами для СРД. Поэтому управление комплексом ПСрЗИ (КПСЗ) (параметрический синтез программных СЗИ (ПСЗИ)) подразделяется на управление СРД и управление обеспечивающими средствами для СРД. Последнее, в свою очередь, подразделяется на управление четырьмя подсистемами, которые входят в состав ПСЗИ согласно [8]:

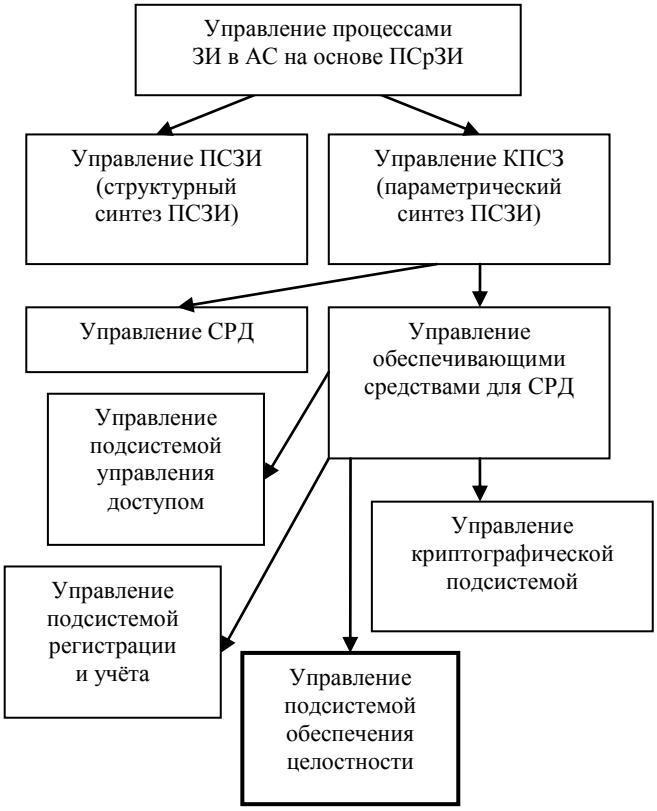
управления доступом;

регистрации и учёта;

криптографической;

обеспечения целостности.

Одной из базовых задач управления процессами ЗИ в АС на основе ПСрЗИ является задача управления контролем целостности рабочей среды АС, относящаяся к управлению подсистемой обеспечения целостности. Данная задача, принадлежащая нижнему уровню управления процессами ЗИ (контуру управления КПСЗ) и являющаяся частным случаем более общей задачи оптимизации контроля защищённости информации, состоит в следующем.



Структура задач управления процессами ЗИ в АС на основе ПСрЗИ

Своевременное обнаружение нарушения защищённости информации существенно снижает риски при выполнении АС своих задач по прямому назначению. При этом поддержание защищённости информации на требуемом уровне должно осуществляться путём периодического контроля параметров функционирования как самой ПСЗИ, так и защищаемой информации, и выполнения в случае необходимости соответствующих операций по компенсации нарушений защищённости.

Необходимость проведения контроля целостности отмечается в Руководящих документах Гостехкомиссии РФ. Так, в п. 6.3 «Концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» среди функций, выполняемых обеспечивающими средствами для СРД, указывается функция контроля целостности программной и информационной части как самой СРД, так и обеспечивающих её средств [7].

Данное требование реализуется в конкретных сертифицированных ПСрЗИ. Для примера рассмотрим СЗИ от НСД в ПЭВМ «Спектр-Z» [9]. К числу её основных функциональных характеристик относится такая возможность системы, как контроль целостности программного обеспечения. Система «Спектр-Z» является многоуровневой системой защиты, причём третий уровень её функционирования представляет собой контроль целостности системы «Спектр-Z» и средств вычислительной техники (СВТ), который реализуется двумя подсистемами: подсистемой обеспечения целостности рабочей среды ПЭВМ и подсистемой регистрации и учёта работ. Подсистема обеспечения целостности рабочей среды ПЭВМ характеризуется следующими функциональными возможностями:

– периодическим контролем за целостностью системы «Спектр-Z» автоматически (в период загрузки и окончания работы СВТ) и вручную (во время процесса работы в СВТ);

– возможностью автоматического восстановления системных компонент;

– антивирусными возможностями.

Даже при сложных нарушениях в работе ПЭВМ система «Спектр-Z» поможет самостоятельно и быстро восстановить рабочую среду.

Под целостностью рабочей среды ПЭВМ понимается первоначальное (на момент инсталляции системы «Спектр-Z») состояние основных компонентов компьютера: CMOS, MBR, CONFIG.SYS, AUTOEXEC.BAT, загрузочного раздела, системных и прикладных программ, данных. В случае корректировки основных компонентов компьютера под эталонным состоянием рабочей среды ПЭВМ понимается фиксируемое состояние компьютера на текущий момент.

В процессе инсталляции «Спектр-Z» анализируется и фиксируется состояние специального программного обеспечения (СПО) компьютера, которое в дальнейшем принимается как эталонное, а, следовательно, должно контролироваться и поддерживаться. Поэтому при инсталляции необходимо обеспечить создание на ПЭВМ эталонной рабочей среды. Подсистема обеспечения целостности рабочей среды фиксирует:

– обнаружение несанкционированных изменений в СПО компьютера со стороны лиц, получивших доступ к ПЭВМ;

– обнаружение несанкционированных изменений, вызванных компьютерными вирусами и программами-вредителями;

– обнаружение искажений в программах и ключевой информации, возникших в результате машинных сбоев или износа магнитного носителя.

Подсистема обеспечения целостности контролирует состояние оперативной памяти ПЭВМ, содержание главной корневой записи диска и загрузочного сектора, состояние батарейной памяти CMOS, файлы конфигурирования и автозапуска CONFIG.SYS и AUTOEXEC.BAT, системные и прикладные программы и данные. Подсистема обеспечения целостности фиксирует действия вирусов (как известных, так и новых) и предоставляет возможность восстановления состояния среды в соответствии с эталоном. Она также выполняет автоматическое восстановление основных компонентов рабочей среды ПЭВМ, а в случае невозможности автоматического восстановления сигнализирует об этом пользователю, выдавая данные о повреждённых частях СПО ПЭВМ для проведения ручного восстановления.

Для запоминания СПО запускается программа. В процессе работы с ней на дисплей выдаётся меню настройки, в котором выбираются конкретные контролируемые параметры. После произведённого выбора происходит запоминание текущего состояния выбранных параметров. Проверка чистоты среды осуществляется запуском тестовой программы. При этом, если запускается Спектр-Z.EXE/a, то осуществляется автоматическое восстановление изменённых файлов, после чего выводится сообщение об итогах попытки восстановления. Запуск подсистемы поддержания целостности выполняется автоматически в период загрузки операционной системы, но, кроме того, предусматривается возможность выполнения пользователем контрольного тестирования и по своей инициативе вызова главной тестовой программы. Процесс тестирования можно прекратить одновременным нажатием клавиш Ctrl и Break.

Таким образом, на примере организации контроля целостности СПО в системе «Спектр-Z» видно, что такой контроль предполагает необходимость оптимизации управления двумя основными группами параметров (управляемых параметров функционирования подсистемы обеспечения целостности рабочей среды):

параметров, задающих временную последовательность проведения контрольных проверок;

параметров, задающих эталонное состояние СПО (контролируемых параметров).

Последняя группа параметров может существенно варьироваться. Так, меню настройки подсистемы поддержания целостности рабочей среды системы «Спектр-Z», предназначенное для выбора этих параметров, содержит следующие пункты:

- CMOS;
- AUTOEXEC.BAT;
- CONFIG.SYS;
- главная корневая запись;
- резиденты;
- операционная среда;
- рабочие программы;
- наборы данных.

Если были выбраны пункты «Операционная среда», «Рабочие программы», «Наборы данных», то на каждый такой пункт меню производится запрос для выбора групп файлов.

Очевидно, что проведение контроля целостности СПО связано с определёнными временными затратами. Суммарные временные затраты на эти цели тем больше, чем чаще проводятся контрольные проверки и чем больше задаётся контролируемых параметров. При этом объём контролируемых параметров существенно влияет на полноту контроля, а периодичность проведения контрольных проверок — на время пребывания АС в состоянии необнаруженного нарушения целостности рабочей среды. Стремление сократить число контрольных проверок целостности рабочей среды и связанные с ними временные затраты, с одной стороны, и требование обеспечить своевременное обнаружение нарушения целостности рабочей среды — с другой, вызывает необходимость построения оптимальной стратегии контроля.

Пусть $0;\bar{T}$ — общий планируемый период контроля целостности рабочей среды. В некоторые моменты времени τ_k начинается проведение контрольных проверок целостности рабочей среды, в результате которых выясняется, произошло ли нарушение целостности СПО к моменту проверки. При обнаружении в момент времени t нарушения целостности выполняются работы по её восстановлению, после чего осуществляется перепланирование контрольных проверок на новый планируемый период $t;\bar{T}$. Таким образом, оперативное планирование контроля производится на временных интервалах между контрольными проверками.

Постановка задачи строится на следующих предположениях [1].

1. О нарушениях целостности СПО становится известно только в результате контрольных проверок.

2. Контрольные проверки не изменяют собственных характеристик защищённости АС.

3. АС не может подвергнуться нарушению целостности СПО во время проведения контрольных проверок.

4. Длительность проведения контрольной проверки определяется выбранным набором контролируемых параметров.

5. При обнаружении нарушения целостности СПО осуществляется её восстановление и перепланирование контрольных проверок.

6. Последняя из возможных проверок осуществляется в момент времени T.

Требуется найти такое правило проведения контрольных проверок, которое обеспечивало бы наилучшее качество функционирования ПСЗИ. Искомое правило должно определять как момент времени проведения очередной планируемой контрольной проверки, так и набор контролируемых параметров.

Таким образом, в статье на основе проведённого анализа проблемы управления контролем целостности СПО АС, являющейся одной из базовых проблем организационно-технологического управления процессами ЗИ, поставлена конкретная задача управления контролем целостности на базе автоматизации запуска главной тестовой программы подсистемы контроля целостности, что обеспечит максимальный уровень защищённости при минимизации негативного влияния ПСЗИ на эффективность функционирования АС по прямому назначению.

ЛИТЕРАТУРА

1. Методологические основы безопасности использования ИТ в системах электронного документооборота: монография / И.И. Застрожнов [и др.]. — Воронеж: Научная книга, 2011. — 252 с.

2. Герасименко В.Г. Информация и безопасность // Региональный научно-технический вестник. — Воронеж: ВГТУ, 1999. Вып. 4. — С. 66—67.

3. ГОСТ 50.922-96. Стандартизованные термины и определения в области защиты информации.

4. Гаценко О.Ю. Защита информации. Основы организационного управления. — СПб.: Сентябрь, 2001. — 228 с.

5. Гостехкомиссия РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. — М., 1992.

6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: в 2 кн.: Кн. 1. — М.: Энергоатомиздат, 1994. — 400 с.

7. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. — М., 1992.

8. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М., 1992.

9. Государственная система защиты информации. Система «Спектр-Z»: Техническая документация. — М.: Государственный научно-исследовательский институт моделирования интеллектуальных сложных систем, 1995. — 70 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.
Воронежский институт МВД России
E-mail: idrovnikova@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473)262-32-78.

Кабанов Дмитрий Александрович. Преподаватель.
В/Ч 28683
E-mail: inselutin@gmail.com
Россия, 394042, г. Воронеж, ул. Минская, 2. Тел. (473)223-27-40

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems. Doctor of technical sciences, assistant professor.
Voronesh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473)262-32-78.

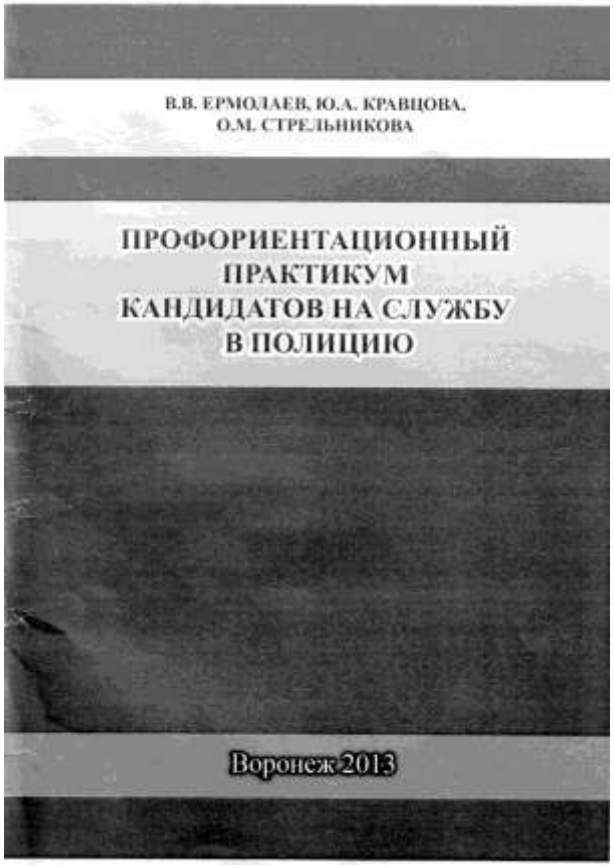
Kabanov Dmitry Alexandrovich. Lecturer.
Military division № 28683.
Work address: Russia, 394042, Voronezh, Minskaya Str., 2. Tel. (473)223-27-40.

Ключевые слова: информационная безопасность; автоматизированные системы; специальное программное обеспечение.

Key words: information security; automated systems; special software.

УДК 621.3

ИЗДАНИЯ ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ



Ермолаев В.В.

Профориентационный практикум кандидатов на службу в полицию / В.В. Ермолаев, Ю.А. Кравцова, О.М. Стрельникова. — Воронеж: Воронежский институт МВД России, 2013. — 114 с.

В практикуме предлагаются популярные психологические методики по самодиагностике при выборе профессии для определения склонностей, способностей, интересов, личностных качеств, уточнения профессиональных планов. Подробно описаны разные группы активизирующих профориентационных игр и упражнений. Приводятся советы по снятию экзаменационного стресса и упражнения для поддержания работоспособности в период подготовки к вступительным испытаниям в вузы.

Методические материалы практикума предназначены для выпускников средних образовательных учреждений, абитуриентов, студентов вузов, их родителей, а также специалистов, занимающихся профориентационной работой.

А.А. Рогожин

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО СТРУКТУРНО-ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ НАДЕЖНОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ: ФОРМАЛИЗОВАННАЯ ПОСТАНОВКА ЗАДАЧИ

APPLICATION OF TECHNOLOGY OF THE AUTOMATED STRUCTURAL AND LOGICAL MODELLING FOR THE QUANTITATIVE ESTIMATION OF RELIABILITY OF THE INTEGRATED SYSTEMS OF SAFETY: THE FORMALIZED PROBLEM DEFINITION

Использован общий логико-вероятностный метод системного анализа и технология автоматизированного структурно-логического моделирования надежности и безопасности структурно-сложных технических систем. Сформирован перечень оцениваемых показателей надежности интегрированной системы безопасности. Разработана структурно-логическая модель (схема функциональной целостности) интегрированной системы безопасности. Задан логический критерий функционирования интегрированной системы безопасности.

The general logical and probabilistic method of the system analysis and technology of the automated structural and logical modelling of reliability and safety of structural and difficult technical systems is used. The scheme of functional integrity (structural and logical model) integrated system of safety is developed. The list of estimated indicators of reliability of the integrated system of safety is created. The logical criterion of functioning of the integrated system of safety is set.

Введение.

При разработке математической модели оценки надежности интегрированной системы безопасности (ИСБ) будет использована единая методика общего логико-вероятностного метода моделирования (ОЛВМ), которая характеризуется следующими основными этапами:

- принятие и формулировка основных ограничений и допущений;
- формирование перечня оцениваемых показателей надежности ИСБ;
- определение структурной схемы ИСБ в минимальной конфигурации для формализованной постановки задачи моделирования оценки ее надежности;
- формализованная постановка задачи моделирования и расчета, включающая в себя разработку структурно-логической модели (схемы функциональной целостности) ИСБ и задание логического критерия ее функционирования (ЛКФ);
- построение логической математической модели (логической функции) работоспособности ИСБ (прямой подход) с помощью программного комплекса «АРБИТР»;
- построение расчетной вероятностной модели, позволяющей количественно оценить исследуемое свойство надежности ИСБ с помощью программного комплекса «АРБИТР»;
- определение исходных данных (вероятностных, временных параметров элементов ИСБ) и расчет оцениваемых показателей надежности с помощью программного комплекса «АРБИТР», анализ полученных данных.

1. Основные ограничения и допущения при моделировании оценки надежности ИСБ.

При моделировании оценки надежности ИСБ приняты следующие ограничения и допущения:

– Интегрированная система безопасности (ИСБ) – это совокупность совместно действующих подсистем как правило, СОТС (система охранно-тревожной сигнализации), СПС (система пожарной сигнализации), СОТ (система охранная телевизионная), СКУД (система контроля и управления доступом), СУЖ (система управления жизнеобеспечением), предназначенная для обеспечения противокриминальной и антитеррористической защиты объекта, в том числе в безоператорном режиме [2].

– Независимость в совокупности отказов всех элементов исследуемых подсистем и проектируемой ИСБ в целом. Отказы отдельных элементов возникают по причинам их естественного старения, что обычно не зависит от состояний других элементов системы. Поэтому данное допущение для проектной оценки надежности ИСБ может быть принято.

– Все структурные элементы в ИСБ восстанавливаются. Неограниченность процессов восстановления отказавших элементов. Это означает, что в процессе эксплуатации ИСБ восстановление элементов начинается сразу после момента их отказа и осуществляется с постоянной интенсивностью, независимо от числа одновременно отказавших элементов в системе. Это положение допустимо, поскольку в проектируемой ИСБ все элементы высоконадежные, а интенсивности их восстановления на много порядков выше интенсивности отказов. В этом случае одновременный отказ двух и более элементов на небольшом интервале времени восстановления крайне маловероятен и им можно пренебречь. Следовательно, независимость и неограниченность восстановлений отказавших элементов в проектируемой ИСБ обеспечивается даже небольшим количеством обслуживающего персонала.

– В расчетах считается, что случайные величины времени безотказной работы и времени восстановления всех элементов ИСБ распределены по экспоненциальному закону. Для простых элементов (без собственного внутреннего резервирования) эти допущения вполне приемлемы.

– Все средства подключения резервных элементов (если таковые имеются) считаются абсолютно надежными. Это положение считается допустимым, поскольку в проектируемой ИСБ все функции переключения резервов относительно простые.

– Допускается не использовать локальный контроллер в исследуемой структуре ИСБ, функцию управления будет выполнять исключительно сервер. Такое допущение может быть принято, так как в большинстве современных ИСБ существует возможность передачи информации от подсистем на верхний уровень иерархии напрямую, посредством преобразователей интерфейсов.

– Допускается, что изменение показателей надежности некоторых элементов ИСБ не оказывает существенного влияния на надежность всей ИСБ.

2. Формирование перечня оцениваемых показателей надежности ИСБ.

Коэффициент готовности.

В соответствии с положениями [1] объективным показателем надежности как технических подсистем так и ИСБ в целом, является комплексный показатель — коэффициент готовности (Кг) к выполнению целевой функции.

Целевой функцией ИСБ является противокриминальная и антитеррористическая защита объектов.

Коэффициенты готовности по техническим подсистемам и/или для ИСБ в целом определяют по формуле:

$$K_Г = \frac{T_0}{T_0 + T_B}, \quad (1)$$

где T_0 — контрольное время обеспечения работоспособности ИСБ, ч;

T_B — активное время восстановления работоспособности ИСБ после отказа(ов) (без учета подготовительно-заключительного времени), ч.

Согласно [1] расчетное значение Кг не должно быть менее 0,93. По конкретным условиям применения и эксплуатации ИСБ на объекте допустимое значение времени То указывают в эксплуатационной технической документации на ИСБ. Допустимое значение времени T_B определяется расчетом с учетом значения Кг или устанавливается обслуживающей организацией в зависимости от наличия обменного фонда, запасных частей, обеспеченности инструментами, расходными материалами и времени прибытия электромонтеров на объект для восстановления работоспособного состояния отказавших ТСО. Для практического обеспечения допустимого значения T_B применяют следующие формы проведения восстановительных работ: ремонт без демонтажа; ремонт с демонтажом и последующим восстановлением в ремонтном подразделении, а затем с возвратом для повторного монтажа.

Следовательно, для проектной оценки надежности ИСБ можно обоснованно рассчитывать Кг ИСБ и сравнивать с регламентированным ГОСТ значением Кг гост = 0,93.

Показатели роли элементов ИСБ.

В системных исследованиях характеристики значимостей и вкладов элементов в общую надежность ИСБ играют особую и очень важную роль. Они позволяют количественно оценить, какую роль играет надежность отдельных элементов в реализации надежности всей ИСБ в целом и на сколько изменение параметров надежности отдельных элементов может изменить общую системную характеристику надежности $Р_{исб} = Кг_{исб}$. Поэтому, по своему физическому смыслу показатели значимости и вкладов должны выполнять важную прогностическую функцию в системном анализе и обеспечивать решение различных оптимизационных задач, задач параметрического и структурного синтеза, выработки эффективных и научно обоснованных решений, направленных на повышение надежности ИСБ охраняемых объектов.

Рассмотрим три показателя роли отдельных элементов — значимость, положительный вклад и отрицательный вклад, которые широко используются в ОЛВМ.

В самом общем случае определение значимости ξ_i отдельного элемента *i* ИСБ следующее:

$$\xi_i = \frac{P_{исб}}{P_i = 1} - \frac{P_{исб}}{P_i = 0};\ i=1,2,\ldots,H, \qquad (2)$$

где $\frac{P_{исб}}{P_i = 1}$ — значение вероятностной характеристики ИСБ при абсолютной надежности элемента *i*;

$\frac{P_{исб}}{P_i = 0}$ — значение вероятностной характеристики ИСБ при достоверном отказе элемента *i* на рассматриваемом интервале *t* времени функционирования.

Анализ определений значимости элементов (2) позволяет сделать следующие выводы:

1. Величина ξ_i отдельного элемента *i* точно равна изменению значения системной характеристики $P_{исб}$ (в нашем случае — $Kг_{исб}$) вследствие изменения собственного параметра P_i от 0 до 1 и фиксированных значениях параметров всех других элементов ИСБ.

2. Диапазон значений вероятностного показателя значимости составляет [−1,0,+ 1] включительно.

3. Отрицательное значение $\xi_i < 0$ характеризует «вредное влияние» элемента *i* на ИСБ. В этом случае увеличение показателя надежности самого элемента *i* безусловно приводит к уменьшению надежности всей ИСБ в целом, а точнее — рассматриваемого режима ее функционирования. Отрицательные значимости элементов характерны для немонотонных логико-вероятностных моделей ИСБ.

4. Нулевое значение характеристики значимости $\xi_i = 0$ означает, что данный элемент *i* оказывает несущественное влияние на реализацию рассматриваемого режима функционирования ИСБ в целом.

5. Положительное значение $\xi_i > 0$ определяет то максимально возможное увеличение показателя надежности ИСБ, которое он может получить, если изменить показатель надежности только одного элемента *i* от 0 до 1 включительно.

6. В отличие от немонотонных ИСБ все элементы монотонных систем могут иметь только положительные или нулевые значения характеристик их значимости.

7. Для случая, когда процессы отказов (или отказов и восстановлений) всех элементов ИСБ являются независимыми в совокупности, значимости (2) элементов ИСБ равны соответствующим частным производным:

$$\xi_i = \frac{\partial P_{исб}}{\partial P_i},\ i=1,2,\ldots,H. \qquad (3)$$

Положительный и отрицательный вклады элементов ИСБ.

Наряду с характеристиками значимости в ОЛВМ системного анализа систем все большее применение начинают находить показатели положительного β_i^+ и отрицательного β_i^- вкладов их элементов, i =1,2,...,H . Дело в том, что показатель значимости ξ_i, по определению, не зависит от текущего значения собственного параметра P_i данного элемента и характеризует влияние на систему только теоретического, максимального, предельно возможного изменения этого параметра от 0 до 1. Однако реальные

возможности изменения собственного параметра элемента могут быть только от текущего значения P_i до 1 и от текущего значения P_i до 0 . Поэтому характеристики вкладов β_i^+ и β_i^- должны определять, на сколько изменится системный показатель надежности $P_{исб}$ при указанных изменениях параметра P_i элемента *i* исследуемой системы. Основные расчетные формулы определения вкладов элементов следующие:

$$\beta_i^+ = \frac{P_{исб}}{P_i = 1} - P_{исб}\,, \tag{4}$$

$$\beta_i^- = -\left(P_{исб} - \frac{P_{исб}}{P_i = 0} \right), \text{ i=1,2,….} \tag{5}$$

Во всех показателях роли элементов положительные значения характеристик означают увеличение $P_{исб}$ при соответствующих изменениях P_i:

от 0 до 1 для ξ_i ;

от P_i до 1 для β_i^+ ;

от P_i до 0 для β_i^- , и наоборот.

При независимости отказов элементов вычисления β_i^+ и β_i^- могут выполняться по формулам (6) и (7):

$$\beta_i^+ = 1 - P_i \tilde{\xi}_i\,, \tag{6}$$

$$\beta_i^- = -P_i \xi_i\,. \tag{7}$$

Из выражений (2), (4), (5) и (6), (7) можно получить следующую формулу:

$$\xi_i = \beta_i^+ - \beta_i^- \tag{8}$$

Из нее видно, что вклады элементов представляют собой доли значимостей, пропорциональные значениям P_i и $1 - P_i$.

Для анализа ИСБ в целях повышения ее надежности наиболее информативной представляется характеристика положительного вклада элементов. Она представляет те реальные возможности по изменению параметров элементов, которые могут оказать наиболее существенное практическое влияние на увеличение надежности исследуемой ИСБ в целом. Например, если P_i близка к 1, то даже при большой значимости этого элемента его реальный вклад в увеличение основного показателя надежности системы может оказаться крайне незначительным, что и покажет β_i^+ .

3. Определение универсальной структурной схемы ИСБ в минимальной конфигурации и задание показателей надежности элементов.

При разработке математической модели оценки надежности на этапе проектирования необходимо учитывать инвариантность структур ИСБ для одного и того же объекта.

Так как структуры ИСБ могут изменяться как по составу элементов, так и целых подсистем, необходимо произвести функционально-структурную декомпозицию и разработать универсальную структурную схему ИСБ в минимальной конфигурации, которую однозначно можно будет использовать для формализованной постановки задачи моделирования оценки надежности ИСБ. Универсальность такой структурной схемы ИСБ обусловлена наличием минимального набора элементов, обеспечивающих выполнение основных функций ИСБ, т.е. функционально необходимых элементов.

Универсальная структурная схема ИСБ в минимальной конфигурации представлена на рис. 1.

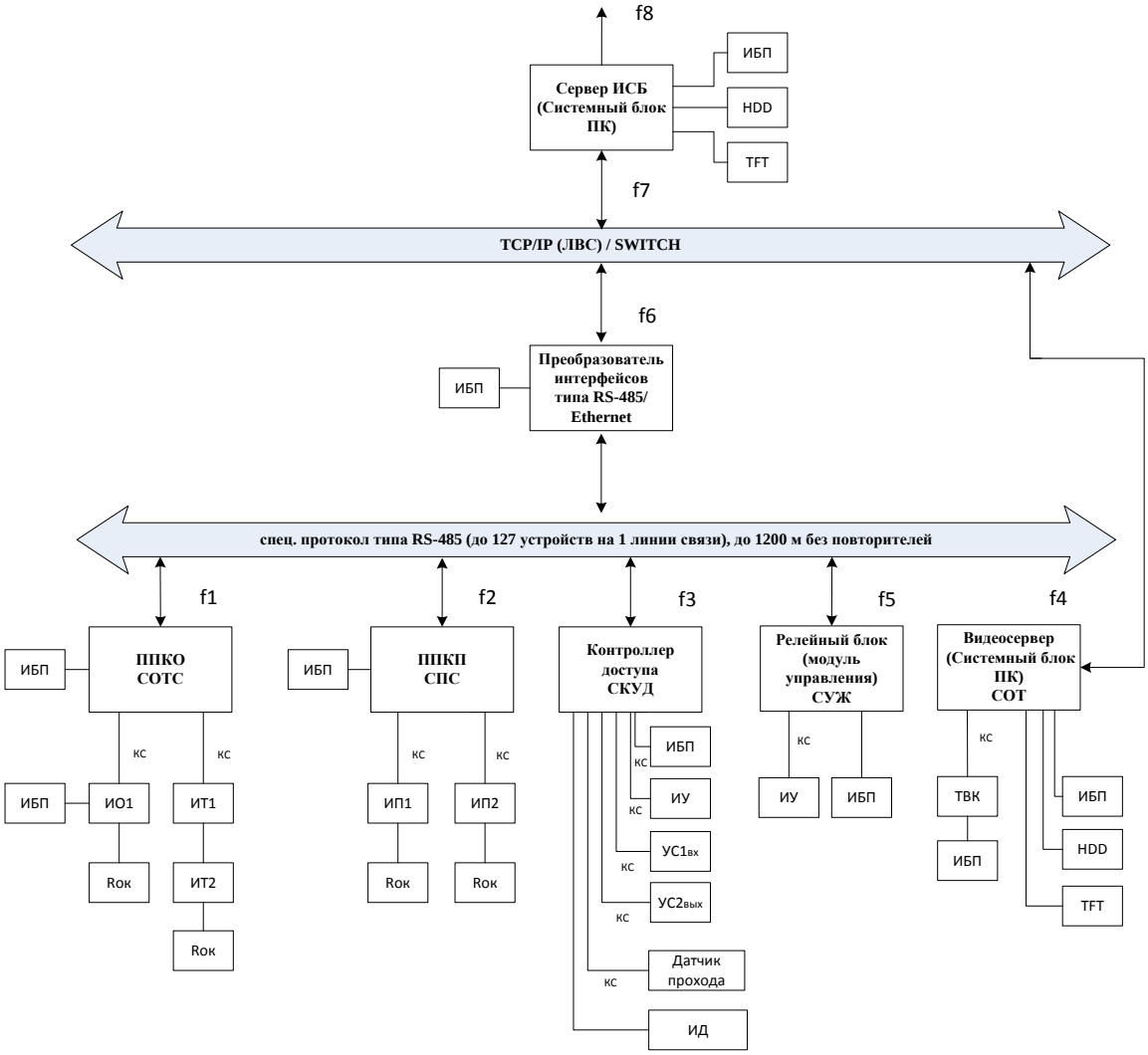


Рис. 1. Универсальная структурная схема ИСБ в минимальной конфигурации

Описание элементов и основных функций f1—f8 универсальной структурной схемы ИСБ в минимальной конфигурации, полученной в результате функционально-структурной декомпозиции, представлены соответственно в табл. 1 и 2.

Необходимо сформулировать логический критерий функционирования (ЛКФ) ИСБ, т.е. при каких условиях ИСБ выполняет целевую функцию.

Объективно ЛКФ ИСБ интерпретируется следующим образом: ИСБ выполняет свою целевую функцию, т.е. ИСБ работоспособна, когда работоспособны все подсистемы: и ДДП, и СПД, и СОТС, и СПС, и СКУД, и СОТ, и СУЖ.

Логическая функция сформулированного ЛКФ будет выглядеть следующим образом:

$$ЛКФ_{f8} = f_1 \wedge f_2 \wedge f_3 \wedge f_4 \wedge f_5 \wedge f_6 \wedge f_7 . \quad (9)$$

Таблица 1

Описание элементов универсальной структурной схемы ИСБ в минимальной конфигурации

№ п/п	Обозначение структурного элемента ИСБ	Наименование структурного элемента ИСБ	Основная функция структурного элемента ИСБ	Условия реализации основной функции структурного элемента ИСБ
1.	$R_{ок}$	Оконечный элемент – резистор, кОм	Сопротивление току в шлейфе сигнализации (обязательное)	Безотказность самого резистора
2.	ИО	Извещатель охранный	Обнаружение опасности (проникновения на охраняемый объект) и формирование состояния тревоги (путем размыкания, замыкания контактов выходного реле, либо путем изменения тока в цепи ШС)	1. Безотказность самого извещателя; 2. Безотказность источника бесперебойного питания (ИБП).
3.	КС	Кабель связи (соединительный кабель/провод/шнур)	1. Передача информации (извещений, сигналов управления). 2. Подача электропитания на средства ИСБ.	Безотказность самого КС
4.	ИТ	Извещатель тревожный (тревожная кнопка или тревожная педаль)	Формирование тревожного извещения (путем размыкания/ замыкания контактов) мануальным (ручным, ножным) способом	Безотказность самого ИТ
5.	ППКО, ППКП	Прибор приемно-контрольный охранный (ППКО) или пожарный (ППКП) или охранно-пожарный (ППКОП) адресный	Прием извещений от извещателей (шлейфов сигнализации) или других ППКОП, преобразование сигналов, выдачи извещений для непосредственного восприятия человеком, дальнейшей передачи извещений, а в некоторых случаях и для электропитания извещателей.	1. Безотказность самого ППКО/ППКП. 2. Безотказность источника ИБП.
6.	ИП	Извещатель пожарный	Обнаружение опасности (пожара, очага возгорания) и формирование состояния тревоги (путем изменения тока в цепи ШС)	Безотказность самого ИП
7.	ИБП	Источник бесперебойного питания (резервированный, с АКБ)	Бесперебойное электропитание технических средств ИСБ	Безотказность самого ИБП и АКБ
8.	ИУ	Исполнительное устройство типа электромагнитный замок с массой на отрыв М, кг	Приведение устройства преграждающего в открытое/закрытое состояние путем подачи (снятия) эл. тока	Безотказность самого ИУ
9.	$УС1_{вх}$	Считыватель 1	Устройство считывания кода (запоминаемый, вещественный, биометрический код), на входе в контролируемую точку доступа	Безотказность самого $УС1_{вх}$
10.	$УС2_{вых}$	Считыватель 2	Устройство считывания кода на выходе из контролируемой точки доступа	Безотказность самого $УС2_{вых}$
11.	СМК	Магнитоконтактный извещатель типа ИО 102-26 (для металлической двери) или другой датчик прохода	Контролирует положение двери, формирует состояние тревоги (путем размыкания, замыкания выходного контакта).	Безотказность самого датчика прохода

№ п/п	Обозначение структурного элемента ИСБ	Наименование структурного элемента ИСБ	Основная функция структурного элемента ИСБ	Условия реализации основной функции структурного элемента ИСБ
12.	ИД	Идентификаторы	Запоминаемый, вещественный, биометрический код субъекта или объекта доступа	Невозможность копирования идентификатора для НСД.
13.	Контроллер доступа СКУД	Контроллер доступа (устройство управления) адресный	Прием и обработка кода, принятие решения о доступе, предоставление/отказ в доступе путем подачи управляющего сигнала на ЭМЗ)	1. Безотказность самого контроллера доступа; 2. Безотказность ИБП
14.	ИУ	Исполнительное устройство	Исполнительное устройство инженерной системы, которое приводит ее в состояние включено/выключено	1. Безотказность самого ИУ.
15.	Релейный блок (модуль управления) СУЖ	Релейный блок (модуль управления) СУЖ адресный	Подача управляющего сигнала на исполнительное устройство путем замыкания/размыкания выходных контактов реле	1. Безотказность самого релейного блока. 2. Безотказность ИБП.
16.	ТВК	Телевизионная камера (видеокамера СОТ) аналоговая	Формирование видеоизображения (аналогового видеосигнала) из контролируемой зоны и передача по линии связи на видеосервер	1. Безотказность самой ТВК. 2. Безотказность источника бесперебойного питания (ИБП).
17.	Видеосервер (системный блок ПК) СОТ	Видеосервер (системный блок ПК) СОТ	Мультимедийный серверный ПК (с установленной платой видеоввода) с установленным ПО для выполнения функций видеоконтроля, видеоеорегистрации	1. Безотказность самого ПК; 2. Безотказность ИБП.
18.	TFT	Профессиональная TFT-панель (монитор)	Отображение видеоинформации из охраняемых зон	Безотказность самого монитора
19.	HDD	Жесткий диск ПК	Регистрация и хранение видеоинформации	Безотказность самого жесткого диска
20.	RS-485	Промышленный протокол обмена данными	Линия связи между адресными устройствами по протоколу RS-485	Безотказность самого кабеля связи RS-485
21.	Преобразователь интерфейсов типа RS-485/ Ethernet	Преобразователь интерфейсов типа RS-485/Ethernet	Преобразование данных из протокола RS-485 в TCP/IP	1. Безотказность самого преобразователя интерфейсов; 2. Безотказность ИБП.
22.	TCP/IP (ЛВС) / SWITCH	Локальная вычислительная сеть – сеть передачи данных на основе стека протоколов TCP/IP, технология Ethernet, реализованная на базе Switch	Обмен данными между устройствами 1 и 2 уровней иерархии в ИСБ (между подсистемами)	1. Безотказность самого Switch. 2. Безотказность ИБП. 3. Безотказность кабельных сетей.
23.	Сервер ИСБ (Системный блок ПК)	Серверный ПК ИСБ	Интеграция, контроль и управление подсистемами ИСБ, обработка, хранение и предоставление информации о безопасности объекта в заданном виде	1. Безотказность самого ПК; 2. Безотказность ИБП.
24.	TFT	Профессиональная TFT-панель (монитор)	Отображение информации о состоянии подсистем ИСБ, планов помещений и т.д.	Безотказность самого монитора
25.	HDD	Жесткий диск ПК	Регистрация и хранение всей информации о состоянии подсистем ИСБ, баз данных.	Безотказность самого жесткого диска

Таблица 2

Описание основных функций универсальной структурной схемы ИСБ

№ п/п	Наименование функции
f1.	Функция контроля и управления СОТС, а также гарантированной передачи информации на верхний уровень иерархии
f2.	Функция контроля и управления СОТС, а также гарантированной передачи информации на верхний уровень иерархии
f3.	Функция контроля и управления доступом, а также гарантированной передачи информации на верхний уровень иерархии
f4.	Функция видеоконтроля и наблюдения, а также гарантированной передачи видеосигнала на верхний уровень иерархии
f5.	Функция управления жизнеобеспечением, а также гарантированной передачи информации на верхний уровень иерархии
f6.	Функция передачи информации между подсистемами в ИСБ, в том числе преобразования интерфейсов
f7.	Функция сервера ИСБ (интеграции, контроля и управления подсистемами безопасности, обработки, хранения и предоставлении информации о безопасности объекта в заданном виде)
f8.	Функция готовности ИСБ к выполнению целевой функции по антитеррористической и противокриминальной защите объектов

Только при таком «жестком» ЛКФ возможна реализация различных сценариев действий одних подсистем ИСБ на события, возникающие в других [2], т.е. достигается самый высокий уровень интеграции, эффективности работы.

Далее определяются временные и вероятностные показатели надежности элементов из сопутствующей технической документации на конкретные изделия.

Решив задачу подготовки исходных данных, непосредственно строим СФЦ ИСБ и вручную вводим в ПК «АРБИТР» [4,5].

4. Разработка структурно-логической модели (схемы функциональной целостности) ИСБ в минимальной конфигурации.

Структурно-логическая модель — СФЦ — своеобразная знаковая система, графический язык записи формализованных знаний человека о составе и условиях функционирования элементов в исследуемой системе. С одной стороны, этот язык является относительно простым и удобным для разработчика модели и пользователя. С другой стороны, аппарат СФЦ является формальным, т.е. математически строгим, что позволяет достаточно точно представлять в структурной модели все существенные логические связи, отношения и зависимости, обеспечивающие адекватность СФЦ моделируемой системе [3]. В математическом смысле СФЦ — это строгие знания, позволяющие определить состояния системы, в которых она выполняет, и состояния, в которых она не выполняет свое функциональное назначение [3]. Методика построения, изобразительные средства построения и основные фрагменты СФЦ представлены в [3].

Итак, разрабатываемая СФЦ должна однозначно определять либо работоспособное состояние ИСБ (прямой подход), либо состояние ее отказа (обратный подход). В статье будет использован прямой подход к оценке надежности ИСБ, т.е. в соответствующей СФЦ ИСБ будут использованы элементы, обеспечивающие и влияющие на выполнение целевой функции ИСБ, характеризующие работоспособность ИСБ.

Для этого необходимо выделить из вербально-графического описания ИСБ, приведенного выше (см. рис. 1, табл. 1), конечное число элементарных бинарных событий, их точное смысловое описание и отображение в СФЦ функциональными вершинами. Все эти бинарные события должны быть параметрически определимы и в совокупности, с достаточной (согласно принятых допущений и ограничений) точностью, структурно представлять моделируемое свойство надежности ИСБ, а именно коэффициент готовности ИСБ к выполнению целевой функции.

Далее в таблицу сводятся конечное число элементов (функциональных и фиктивных вершин СФЦ), их точное смысловое описание, количественные характеристики (вероятностные и временные) и источники информации о надежности этих элементов, а также ЛКФ для фиктивных вершин. На данном этапе решается вопрос подготовки исходных данных для моделирования и дальнейшего расчета $Кг_{исб}$.

Для восстанавливаемых элементов ИСБ в СФЦ (структурных элементов или технических средств ИСБ) задается среднее время наработки на отказ $Тср_i$, [час] и среднее время восстановления $Тв_i$, [час].

Для ИСБ в минимальной конфигурации (рис. 1) с учетом принятых условий реализации основных функций структурных элементов, число элементов в СФЦ ИСБ составит — H = 42.

В результате ввода исходных данных в ПК «АРБИТР» получена СФЦ ИСБ в минимальной конфигурации для моделирования и расчета коэффициента готовности $КГ_{исб}$ при $ЛКФ_{f8}$, которая показана на рис. 2.

Используя разработанную СФЦ и задав параметры надежности элементов, можно осуществить дальнейшее моделирование и расчет оцениваемых показателей надежности ИСБ.

Заключение.

При количественной оценке надежности интегрированных систем безопасности используется технология автоматизированного структурно-логического моделирования надежности и безопасности структурно-сложных технических систем, основанная на общем логико-вероятностном методе системного анализа и реализованная в программном комплексе «АРБИТР».

В статье формализована задача оценки надежности ИСБ. Сформирован перечень оцениваемых показателей надежности ИСБ: коэффициент готовности (системный показатель надежности), значимости, положительные и отрицательные вклады элементов СФЦ ИСБ в системный показатель надежности. Разработана структурно-логическая модель (схема функциональной целостности) ИСБ, сформулирован и формализован логический критерий функционирования ИСБ.

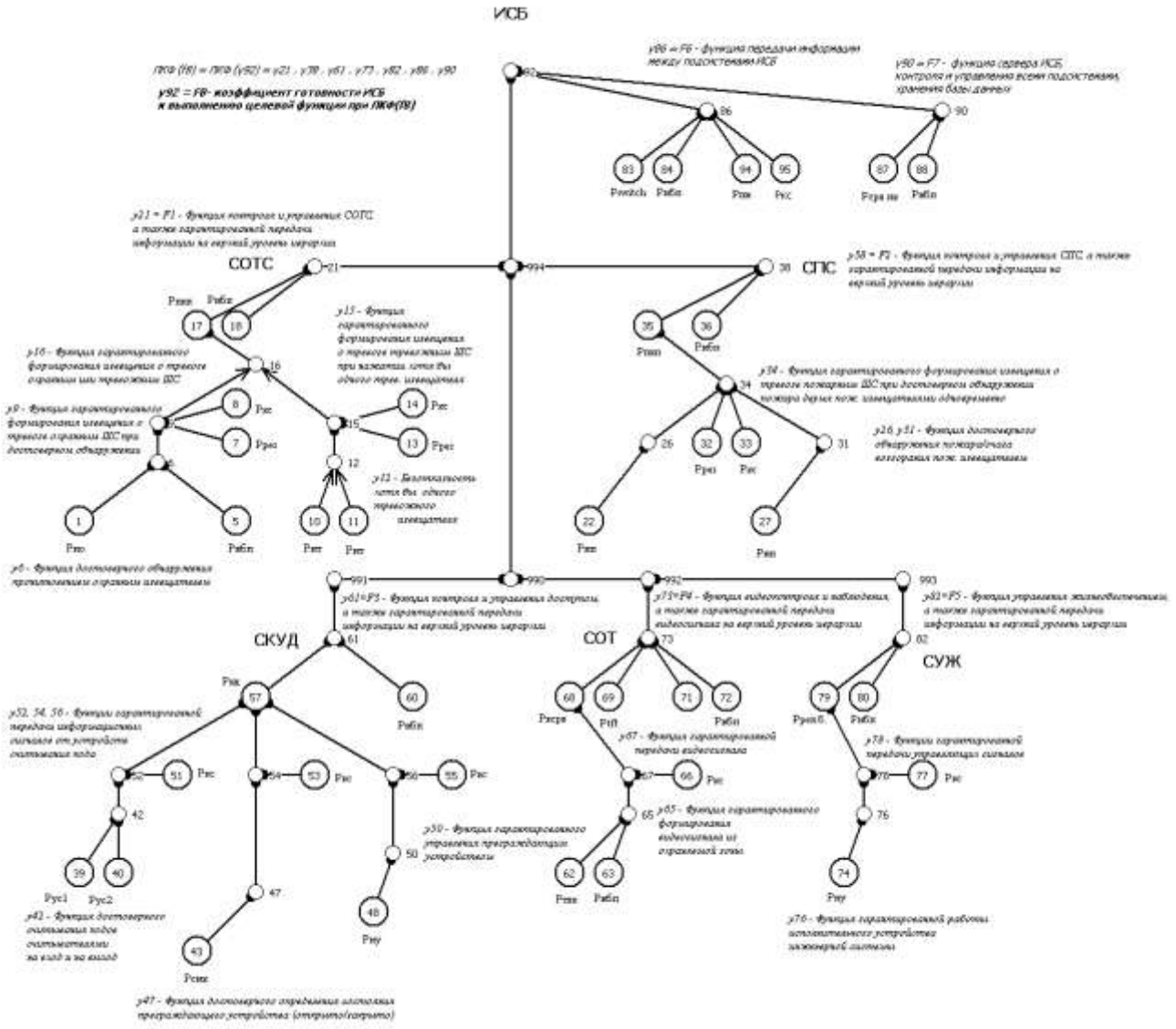


Рис. 2. СФЦ ИСБ в минимальной конфигурации для моделирования $КГ_{исб}$ при ЛКФ = f_8

ЛИТЕРАТУРА

1. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования.

2. Рогожин А.А. Основы построения интегрированных систем безопасности: учебное пособие. — Воронеж: Воронежский институт МВД России, 2012. — 74 с.

3. Можаев А.С., Громов В.Н. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем. — СПб.: ВИТУ, 2000. — 145 с.

4. Можаев А.С. Отчет о верификации программного средства «Программный комплекс автоматизированного структурно-логического моделирования и расчета

надежности и безопасности систем» (АРБИТР, ПК АСМ СЗМА, базовая версия 1.0). СПб.: ОАО «СПИК СЗМА», 2007. — 1031 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Рогожин Александр Александрович. Преподаватель кафедры технических систем безопасности.
Воронежский институт МВД России.
E-mail: raa_tsbs@list.ru.
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2-312-412.

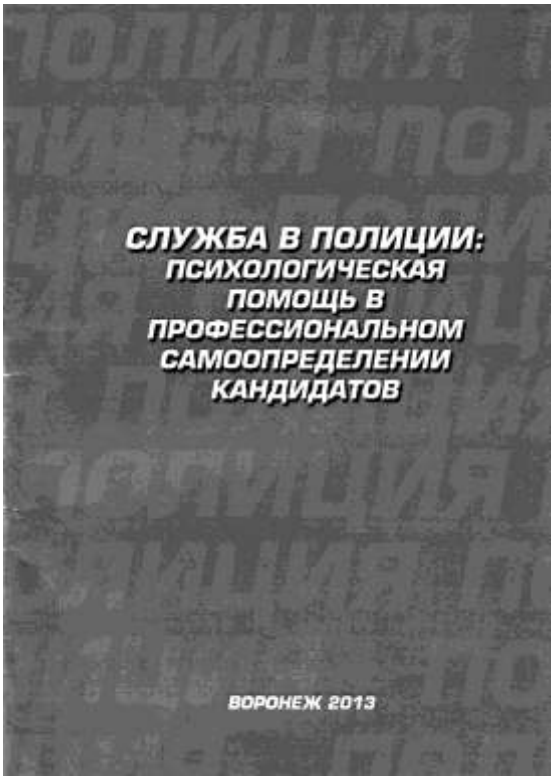
Rogozhin Alexander Alexandrovich. Lecturer of the chair of Technical Security Systems.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2-312-412.

Ключевые слова: интегрированная система безопасности; оценка надежности; общий логико-вероятностный метод; технология автоматизированного структурно-логического моделирования; схема функциональной целостности.

Key words: the integrated system of safety; the general logical and probabilistic method; technology of the automated structural and logical modeling; the scheme of functional integrity; estimation of reliability.

УДК 654.924; 621.38.019.3

ИЗДАНИЯ ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ



Ермолаев В.В.
Служба в полиции: психологическая помощь в профессиональном самоопределении кандидатов: учебное пособие / В.В. Ермолаев, Ю.А. Кравцова, О.М. Стрельникова; под ред. д-ра юрид. наук, проф. А.В. Симоненко. — 2-е изд., исправл. и доп. — Воронеж: ВИ МВД России, 2013. — 100 с.
Изложены современные представления о профессиональном и личностном самоопределении, способы определения степени профпригодности к конкретному виду деятельности посредством всестороннего изучения личности, содержатся рекомендации по выбору профессии.
Приводится профессиографическое описание основных видов деятельности в ОВД и критерии психологической пригодности к ним.
Предназначено для выпускников средних образовательных учреждений, абитуриентов, студентов вузов, их родителей, а также специалистов, занимающихся профориентационной работой.

В.А. Дурденко,
доктор технических наук, доцент,
Воронежский институт инновационных систем

А.А. Рогожин

КОЛИЧЕСТВЕННАЯ ОЦЕНКА НАДЕЖНОСТИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МОДЕЛИРОВАНИЯ

QUANTITATIVE ESTIMATION OF RELIABILITY OF INTEGRATED SYSTEM OF SAFETY ON THE BASIS OF LOGICAL AND PROBABILISTIC MODELLING

С помощью программного комплекса «АРБИТР» построены логическая математическая модель работоспособного состояния интегрированной системы безопасности, вероятностная математическая модель для расчета системных показателей надежности. Приведен пример расчета системного показателя надежности интегрированной системы безопасности — коэффициента готовности, а также значимостей, положительных и отрицательных вкладов всех элементов в общую надежность.

By means of a program complex ARBITR the logical mathematical model of an efficient condition of the integrated system of safety, probabilistic mathematical model for calculation of system indicators of reliability are constructed. The example of calculation of a system indicator of reliability of the integrated system of safety — an availability function, and also importance, positive and negative deposits of all elements to the general reliability is given.

Введение.

Количественная оценка надежности интегрированных систем безопасности (ИСБ) необходима для объективной и научно-обоснованной оценки уровня их безотказности и готовности к выполнению целевых функций по противокриминальной и антитеррористической защите объектов; для разработки планов обеспечения надежности, выработки, обоснования и оптимизации технических решений с учетом их экономической целесообразности на этапах исследования, проектирования и эксплуатации. Оценка надежности ИСБ на стадии проектирования предусмотрена требованиями государственного стандарта [1].

В настоящее время проблема оценки надежности ИСБ [2] является достаточно актуальной ввиду отсутствия научно обоснованного подхода к ее решению.

В статье предлагается для оценки надежности ИСБ использовать программный комплекс (ПК) «АРБИТР», который прошел аттестацию в «Совете по аттестации программных средств» Научно-технического центра по ядерной и радиационной безопасности Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ [4,5]. ПК «АРБИТР» предназначен для автоматизированного моделирования и расчета показателей свойств надежности, стойкости, живучести, устойчивости, технического риска, ожидаемого ущерба и эффективности функционирования структурно-сложных технических систем различных видов, классов и назначения. Выбор в исследовании ПК «АРБИТР» обусловлен также и тем, что в основных режимах моделирования обеспечивается точный расчет показателей надежности, а не приближенных, как в подобных комплексах типа: Risk Spectrum (Швеция), CRISS-4.0 (Россия) и Saphire-7 (США).

В настоящее время ПК «АРБИТР» реализует следующие функции (прошедшие процедуру аттестации в Ростехнадзоре), необходимые для проведения настоящего исследования [4]:

представление в исходной СФЦ (в суперграфе схемы функциональной целостности — СФЦ) до 400 элементов (вершин) и до 100 элементов в каждой декомпозированной вершине (подграфах СФЦ) основного графа исследуемой системы (т.е. можно ввести до 40 000 вершин);

автоматическое построение логических функций, представляющих пути функционирования, сечения отказов или их немонотонные комбинации (явные детерминированные модели исследуемых свойств системы);

автоматическое построение вероятностных функций, обеспечивающих точный расчет показателей устойчивости, эффективности и риска исследуемых систем;

расчет вероятности реализации заданных критериев, представляющих свойства устойчивости, эффективности и риска функционирования систем;

расчет вероятности безотказной работы или отказа и средней наработки до отказа невосстанавливаемых систем;

расчет коэффициента готовности, средней наработки на отказ, среднего времени восстановления и вероятности безотказной работы восстанавливаемых систем;

расчет значимостей, положительных и отрицательных вкладов всех элементов исследуемой системы в вероятность реализации исследуемого свойства, используемые для выработки и обоснования управленческих решений по обеспечению устойчивости, живучести, безопасности, эффективности и риска функционирования;

расчет вероятности реализации отдельных кратчайших путей успешного функционирования (КПУФ) или минимальных сечений отказов (МСО) системы;

учет неограниченного числа циклических (мостиковых) связей между элементами и подсистемами.

Постановка задачи.

В качестве оцениваемых показателей надежности ИСБ предлагается определить (промоделировать и рассчитать):

1. *Комплексный показатель — коэффициент готовности (Кг)* к выполнению целевой функции, согласно [1] Кг гост = 0,93.

2. *Характеристики значимостей* ξ_i *элементов* в «общей надежности» ИСБ (значимость показателя надежности элемента для показателя надежности ИСБ в целом). Ве-

личина ξ_i отдельного элемента i точно равна изменению значения системной характеристики $P_{исб}$ (в нашем случае — $Kг_{исб}$) вследствие изменения собственного параметра P_i от 0 до 1 при фиксированных значениях параметров всех других элементов ИСБ [3];

3. *Положительные* β_i^+ *и отрицательные* β_i^- *вклады элементов* в комплексный показатель — коэффициент готовности $Kг_{исб}$ [3].

Исходные данные для моделирования:

1) СФЦ универсальной структурной схемы ИСБ в минимальной конфигурации (см. рис. 1), которая содержит 42 функциональные вершины, характеризующие бинарные события реализации/нереализации основных функций элементов с заданными вероятностными и временными параметрами.

2) В данной СФЦ ИСБ выполняется 8 базовых функций f1—f8 (см. табл. 1).

3) Системообразующей функцией, определяющей общую надежность ИСБ, является функция f8. Следовательно, логический критерий функционирования [4] ИСБ соответствует реализации функции f8. ЛКФ ИСБ интерпретируется следующим образом: ИСБ выполняет свою целевую функцию, т.е. ИСБ работоспособна, когда работоспособны все ее подсистемы: и дежурно-диспетчерская (ДДП), и сеть передачи данных (СПД), и охранно-тревожной сигнализации (СОТС), и пожарной сигнализации (СПС), и контроля и управления доступом (СКУД), и охранная телевизионная (СОТ), и управления жизнеобеспечением (СУЖ) [2].

Формально ЛКФ ИСБ будет выглядеть следующим образом:

$$ЛКФ_{f8} = f_1 \wedge f_2 \wedge f_3 \wedge f_4 \wedge f_5 \wedge f_6 \wedge f_7, \quad (1)$$

где знак «$\wedge$» — конъюнкция (логическое умножение).

Таблица 1

Базовые функции в исследуемой ИСБ

№	Наименование функции
f1.	Функция контроля и управления охранно-тревожной сигнализацией, а также гарантированной передачи информации на верхний уровень иерархии
f2.	Функция контроля и управления пожарной сигнализацией, а также гарантированной передачи информации на верхний уровень иерархии
f3.	Функция контроля и управления доступом, а также гарантированной передачи информации на верхний уровень иерархии
f4.	Функция видеоконтроля и наблюдения, а также гарантированной передачи видеосигнала на верхний уровень иерархии
f5.	Функция управления жизнеобеспечением, а также гарантированной передачи информации на верхний уровень иерархии
f6.	Функция передачи информации между подсистемами в ИСБ, в том числе преобразования интерфейсов
f7.	Функция сервера ИСБ (интеграции, контроля и управления подсистемами безопасности, обработки, хранения и предоставлении информации о безопасности объекта в заданном виде)
f8.	Функция готовности ИСБ к выполнению целевой функции по антитеррористической и противокриминальной защите объектов

1. Разработка логической модели функционирования ИСБ.

В результате автоматизированного моделирования в ПК «АРБИТР» получена логическая функция работоспособности ИСБ для моделирования и расчета коэффициента готовности $Kг_{исб}$ с учетом $ЛКФ_{f8}$ будет состоять из 3 конъюнкций:

$$Y_{92} = X10\,X13\,X14\,X17\,X18\,X22\,X27\,X32\,X33\,X35\,X36\,X39\,X40\,X43\,X48\,X51\,X53\,X55\,X57\,X60\,X62\,X63\,X66\,X68\,X69\,X71\,X72\,X74\,X77\,X79\,X80\,X83\,X84\,X87\,X88\,X94\,X95 \vee X11\,X13\,X14\,X17\,X18\,X22\,X27\,X32\,X33\,X35\,X36\,X39\,X40\,X43\,X48\,X51\,X53\,X55\,X57\,X60\,X62\,X63\,X66\,X68\,X69\,X71\,X72\,X74\,X77\,X79\,X80\,X83\,X84\,X87\,X88\,X94\,X95 \vee X1\,X5\,X7\,X8\,X17\,X18\,X22\,X27\,X32\,X33\,X35\,X36\,X39\,X40\,X43\,X48\,X51\,X53\,X55\,X57\,X60\,X62\,X63\,X66\,X68\,X69\,X71\,X72\,X74\,X77\,X79\,X80\,X83\,X84\,X87\,X88\,X94\,X95.$$

В полученной логической модели X_i — это бинарное событие реализации/нереализации элементом *i* СФЦ ИСБ своей функции (состояние безотказности/отказа элемента *i*), описание бинарных событий $X_i = i$ приведено в табл. 2.

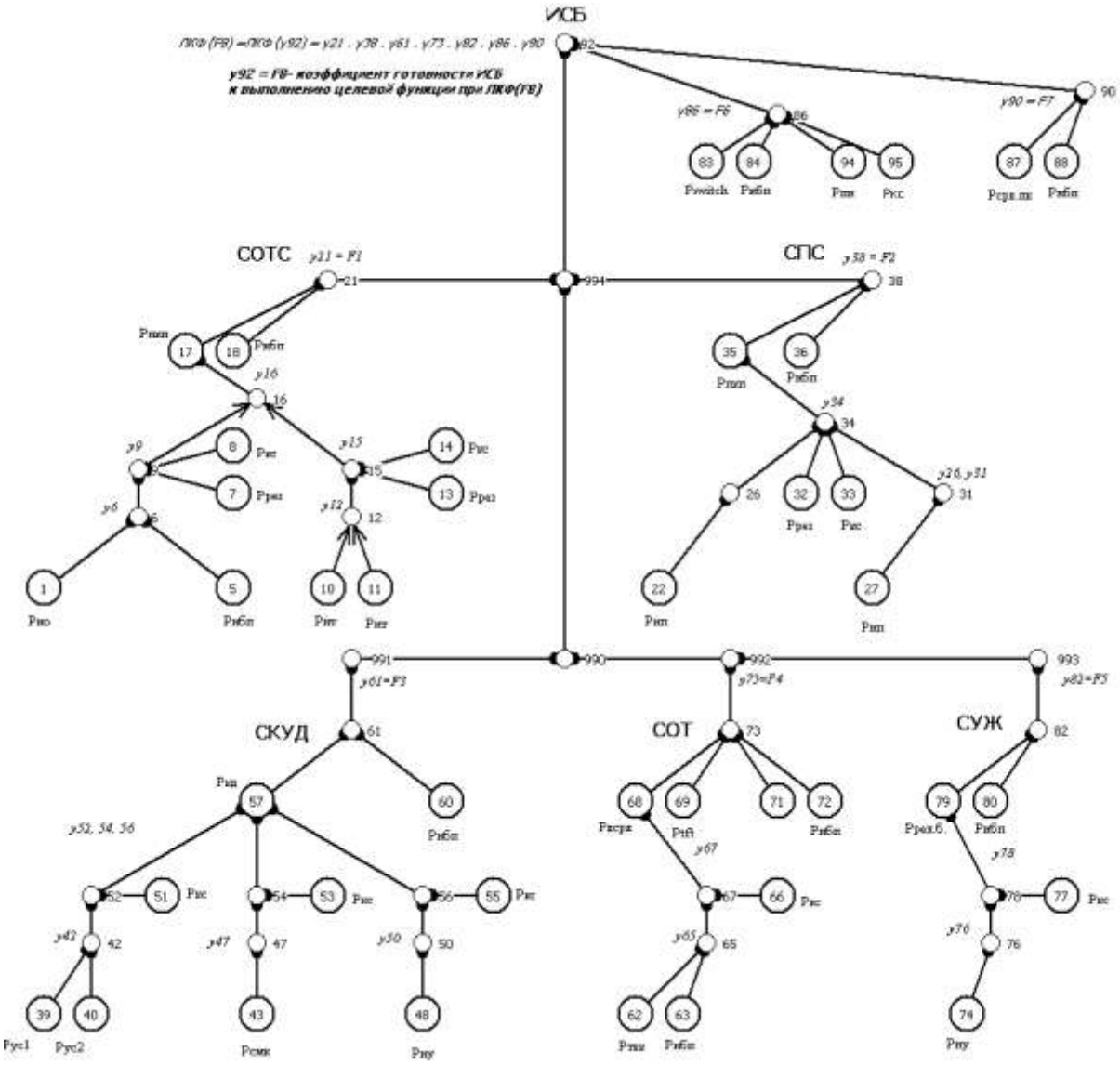


Рис. 1. СФЦ ИСБ в минимальной конфигурации для моделирования $Кг_{исб}$ при ЛКФ = f_8

2. Разработка вероятностной модели функционирования ИСБ.

В результате автоматизированного моделирования в ПК «АРБИТР» преобразована из логической (с помощью специального графоаналитического метода [3]) и получена расчетная вероятностная модель функционирования (работоспособности) ИСБ для расчета коэффициента готовности $Кг_{исб}$ с учетом $ЛКФ_{f8}$, которая будет состоять из 5 одночленов:

$Р_{исб} = Кг_{исб} =$

= Q10 P11 P13 P14 P17 P18 P22 P27 P32 P33 P35 P36 P39 P40 P43 P48 P51 P53 P55 P57 P60 P62 P63 P66 P68 P69 P71 P72 P74 P77 P79 P80 P83 P84 P87 P88 P94 P95 +

+ P1 P5 P7 P8 P17 P18 P22 P27 P32 P33 P35 P36 P39 P40 P43 P48 P51 P53 P55 P57 P60 P62 P63 P66 P68 P69 P71 P72 P74 P77 P79 P80 P83 P84 P87 P88 P94 P95 +

+ P10 P13 P14 P17 P18 P22 P27 P32 P33 P35 P36 P39 P40 P43 P48 P51 P53 P55 P57 P60 P62 P63 P66 P68 P69 P71 P72 P74 P77 P79 P80 P83 P84 P87 P88 P94 P95 -

- P1 P5 P7 P8 P10 P13 P14 P17 P18 P22 P27 P32 P33 P35 P36 P39 P40 P43 P48 P51 P53 P55 P57 P60 P62 P63 P66 P68 P69 P71 P72 P74 P77 P79 P80 P83 P84 P87 P88 P94 P95 -

- P1 P5 P7 P8 Q10 P11 P13 P14 P17 P18 P22 P27 P32 P33 P35 P36 P39 P40 P43 P48 P51 P53 P55 P57 P60 P62 P63 P66 P68 P69 P71 P72 P74 P77 P79 P80 P83 P84 P87 P88 P94 P95.

В полученной вероятностной модели P*i* — это значение собственного вероятностного показателя надежности элемента *i*, в нашем случае, — P*i* =Кг*i* элементов. Значения P*i* =Кг*i* представлены в табл. 2.

Таблица 2

Результаты расчета показателей надежности элементов СФЦ ИСБ при $ЛКФ_{f8}$ в ПК «АРБИТР»

№ элемента *i* СФЦ	T_{oi}, год	P_i = Кг*i*	Значимость ξ_i	Отрицательный вклад β_i^-	Положительный вклад β_i^+	Наименование элемента СФЦ
1	6,849·	0,9999	$1{,}1905\cdot10^{-5}$	$-1{,}1904\cdot10^{-5}$	$1{,}1904\cdot10^{-9}$	Безотказность извещателя охранного (ИО)
5	1,142	0,9994	$1{,}1911\cdot10^{-5}$	$-1{,}1904\cdot10^{-5}$	$7{,}1425\cdot10^{-9}$	Безотказность источника бесперебойного питания (РИБП)
7	114,155	0,99999	$1{,}1904\cdot10^{-5}$	$-1{,}1904\cdot10^{-5}$	$7{,}1425\cdot10^{-11}$	Безотказность резистора (Р)
8	114,155	0,99999	$1{,}1904\cdot10^{-5}$	$-1{,}1904\cdot10^{-5}$	$7{,}1425\cdot10^{-11}$	Безотказность канала связи (кабеля) - КС
10	713,470	1	$6{,}7813\cdot10^{-10}$	$-6{,}7812\cdot10^{-10}$	$6{,}51\cdot10^{-16}$	Безотказность извещателя тревожного (ИТ)
11	713,470	1	$6{,}7813\cdot10^{-10}$	$-6{,}7812\cdot10^{-10}$	$6{,}51\cdot10^{-16}$	Безотказность извещателя тревожного (ИТ)
13	114,155	0,99999	0,00070639	-0,00070638	$4{,}2383\cdot10^{-9}$	Безотказность Р
14	114,155	0,99999	0,00070639	-0,00070638	$4{,}2383\cdot10^{-9}$	Безотказность КС
17	2,055	0,99967	0,99306	-0,99273	0,00033091	Безотказность ППКО
18	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
22	6,849	0,9999	0,99283	-0,99273	$9{,}9273\cdot10^{-5}$	Безотказность извещателя пожарного (ИП)
27	6,849	0,9999	0,99283	-0,99273	$9{,}9273\cdot10^{-5}$	Безотказность извещателя ИП
32	114,155	0,99999	0,99274	-0,99273	$5{,}9564\cdot10^{-6}$	Безотказность Р
33	114,155	0,99999	0,99274	-0,99273	$5{,}9564\cdot10^{-6}$	Безотказность КС
35	2,283	0,9997	0,99303	-0,99273	0,00029782	Безотказность ППКП
36	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
39	11,416	0,99994	0,99279	-0,99273	$5{,}9564\cdot10^{-5}$	Безотказность устройства считывания на вход

№ элемента *i* СФЦ	T_{oi}, год	$P_i = Кг_i$	Значимость ξ_i	Отрицательный вклад β_i^-	Положительный вклад β_i^+	Наименование элемента СФЦ
40	11,416	0,99994	0,99279	-0,99273	$5{,}9564 \cdot 10^{-5}$	Безотказность устройства считывания на выход
43	22,831	0,99997	0,99276	-0,99273	$2{,}9782 \cdot 10^{-5}$	Безотказность датчика прохода
48	2,283	0,9997	0,99303	-0,99273	0,00029782	Безотказность исполнительного устройства (ИУ)
51	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность КС
53	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность КС
55	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность КС
57	2,283	0,9997	0,99303	-0,99273	0,00029782	Безотказность контроллера доступа
60	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
62	2,283	0,9997	0,99303	-0,99273	0,00029782	Безотказность телевизионной камеры (ТВК)
63	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
66	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность КС
68	1,712	0,99997	0,99276	-0,99273	$3{,}3091 \cdot 10^{-5}$	Безотказность видеосервера
69	5,708	0,99988	0,99285	-0,99273	0,00011913	Безотказность видеомонитора (tft-панели)
71	41,976	1	0,99273	-0,99273	$1{,}3499 \cdot 10^{-6}$	Безотказность жесткого диска
72	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
74	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность исполнительного устройства
77	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность КС
79	3,995	0,99983	0,9929	-0,99273	0,00017018	Безотказность релейного блока
80	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
83	6,849	0,9999	0,99283	-0,99273	$9{,}9273 \cdot 10^{-5}$	Безотказность концентратора сети передачи данных (SWITCH)
84	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
87	1,712	0,99997	0,99276	-0,99273	$3{,}3091 \cdot 10^{-5}$	Безотказность сервера ИСБ (ПЭВМ+ПО)
88	1,142	0,9994	0,99333	-0,99273	0,00059564	Безотказность РИБП
94	6,849	0,9999	0,99283	-0,99273	$9{,}9273 \cdot 10^{-5}$	Безотказность преобразователя интерфейсов
95	114,155	0,99999	0,99274	-0,99273	$5{,}9564 \cdot 10^{-6}$	Безотказность канала связи (кабеля)

Подставив вероятностные показатели надежности элементов в полученные расчетные вероятностные модели, всегда можно вычислить нужный системный показатель надежности ИСБ, в нашем случае $Кг_{исб}$, и, соответственно, количественно оценить надежность ИСБ на стадии проектирования.

3. Расчет оцениваемых показателей надежности ИСБ.

В целях апробации полученных математических моделей и, соответственно, расчета показателей надежности исследуемой ИСБ в минимальной конфигурации, а также в качестве примера необходимо выбрать конкретные образцы технических средств ИСБ с известными вероятностно-временными показателями надежности.

В табл. 2 для примера сведены вероятностно-временные показатели надежности элементов СФЦ ИСБ в минимальной конфигурации. Так как ИСБ является полностью

восстанавливаемой системой, для структурных элементов ИСБ также задается время восстановления $T_в$ из отказа в работоспособное состояние. В исследовании примем $T_в$=6 ч.

Результаты расчетов оцениваемых показателей надежности ИСБ

Параметры СФЦ ИСБ:

Число вершин — N = 73 (функциональных и фиктивных).

Число элементов — H = 42 (функциональных).

С помощью ПК «АРБИТР» при ЛКФ$_{f8}$ был рассчитан основной показатель надежности — коэффициент готовности $Кг_{исб}$ к выполнению целевой функции, а также другие важные показатели надежности ИСБ:

$Кг_{исб}$ = 0,9927 — коэффициент готовности ИСБ.

$T_{о\ исб}$ = 745 час (0,08514 год) — средняя наработка на отказ ИСБ.

$T_{в\ исб}$ = 5,46053 час — среднее время восстановления ИСБ.

$W_{исб}$ = 11,745840 — частота (средняя интенсивность) отказов (1/год) ИСБ.

$Q_{исб}(1000)$ = 0,738377 — приближенная вероятность отказа ИСБ.

$P_{исб}(1000)$ = 0,2616 — вероятность безотказной работы восстанавливаемой ИСБ.

Результаты расчета показателей надежности и значимостей элементов СФЦ ИСБ приведены в табл. 2.

Графическое представление полученных данных отображено на рис. 2—5.

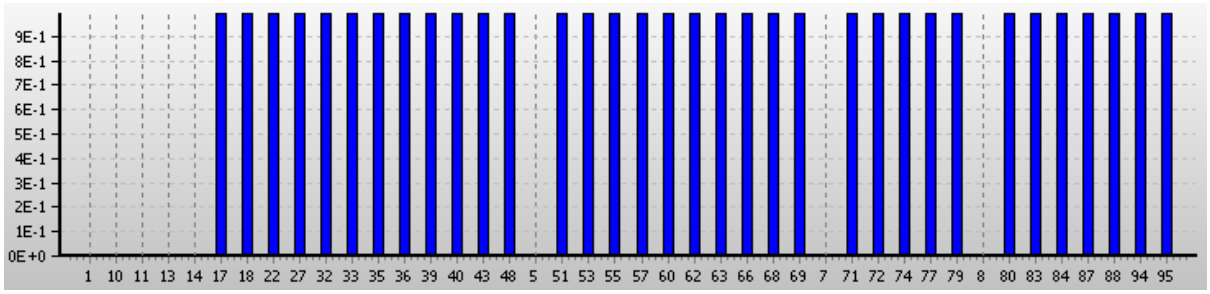


Рис. 2. Диаграмма значимостей элементов ИСБ для $Кг_{исб}$ с учетом ЛКФ$_{f8}$

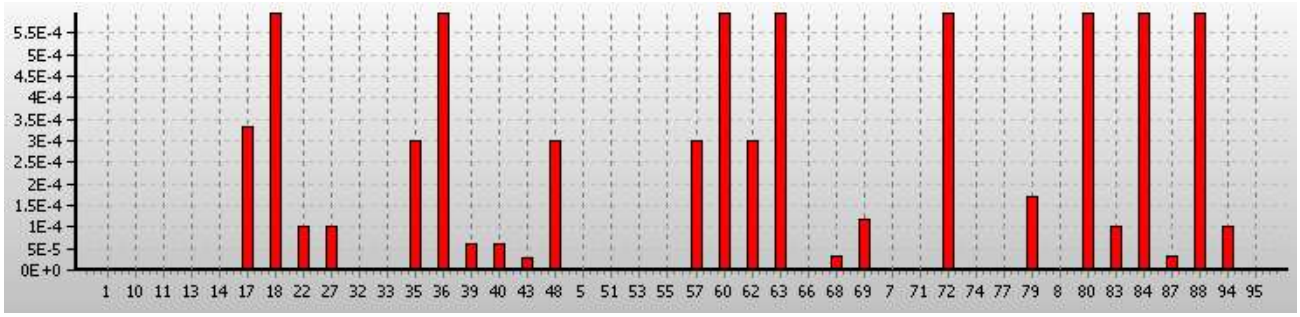


Рис. 3. Диаграмма положительных вкладов элементов ИСБ в $Кг_{исб}$ с учетом ЛКФ$_{f8}$

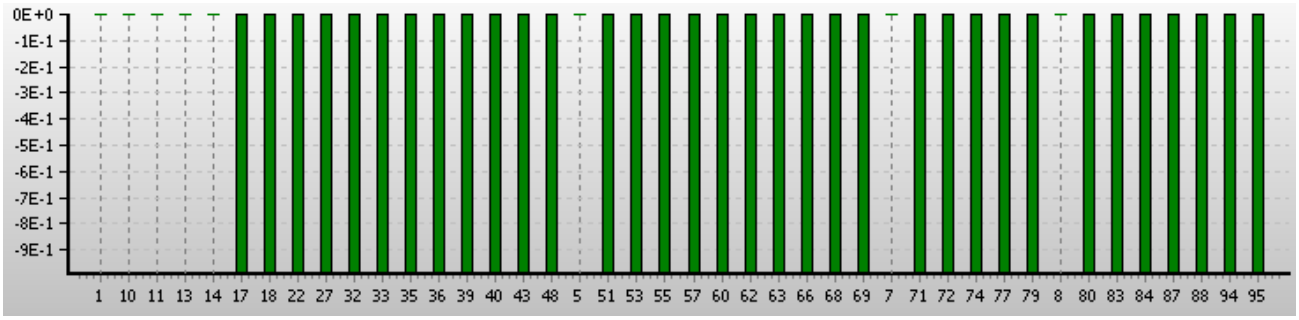


Рис. 4. Диаграмма отрицательных вкладов элементов ИСБ в $Кг_{исб}$ с учетом $ЛКФ_{f8}$

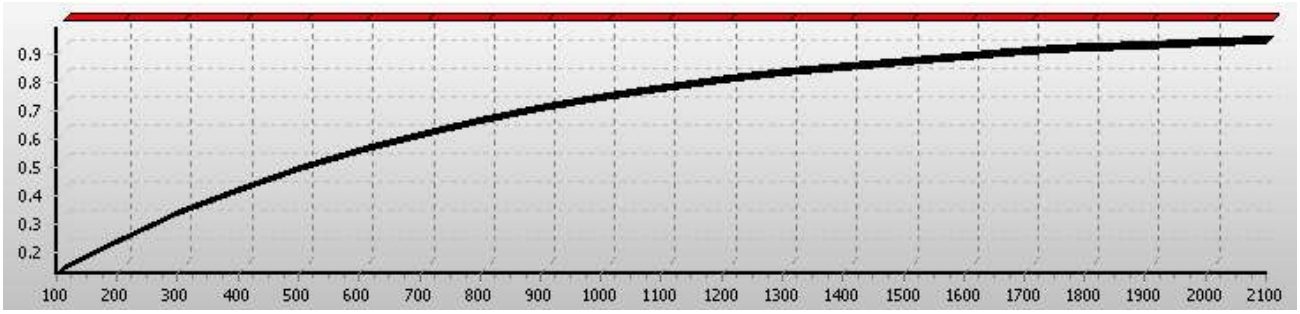


Рис. 5. График функции готовности ИСБ для $Кг_{исб}$ и вероятности первого отказа $Q_{исб}(1000)$ с учетом $ЛКФ_{f8}$

В результате анализа полученных данных можно сделать вывод о соответствии предложенной структуры ИСБ требованиям ГОСТ с точки зрения надежности. Действительно, выполняется условие:

$$Кг_{исб} > Кг_{исб\ гост},$$

т.е. рассчитанное значение коэффициента готовности $Кг_{исб} = 0{,}9927$ больше значения, установленного ГОСТ Р 53704-2009, $Кг_{исб\ гост} = 0{,}93$.

Рассчитанные показатели значимостей и вкладов элементов в системный показатель надежности $Кг_{исб}$ дают детальное представление об уязвимых элементах, надежность которых существенно влияет на общую надежность исследуемой ИСБ. Например, если повысить значение коэффициента готовности элемента 17 (ППКО) от текущего значения 0,99967 до 1, то значение коэффициента готовности ИСБ в целом увеличится незначительно на величину 0.0003, что видно из табл. 2 по полученному положительному вкладу. И наоборот, если уменьшить значение коэффициента готовности элемента 17 (ППКО) от текущего значения 0,99967 до 0, то значение коэффициента готовности ИСБ в целом значительно уменьшится на величину –0.99273, что видно из табл. 2 по полученному отрицательному вкладу.

Заключение.

При количественной оценке надежности интегрированных систем безопасности использована технология автоматизированного структурно-логического моделирования надежности и безопасности структурно-сложных технических систем, основанная на общем логико-вероятностном методе системного анализа и реализованная в программном комплексе «АРБИТР».

На основании принятых допущений и ограничений построена логическая математическая модель функционирования ИСБ, вероятностная математическая модель для расчета системных показателей надежности.

Приведен пример расчета оцениваемых показателей надежности ИСБ и непосредственно оценки надежности ИСБ заданной конфигурации.

ЛИТЕРАТУРА

1. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования.

2. Рогожин А.А. Основы построения интегрированных систем безопасности: учебное пособие. — Воронеж: Воронежский институт МВД России, 2012. — 74 с.

3. Можаев А.С., Громов В.Н. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем. – СПб.: ВИТУ, 2000. —145 с.

4. Можаев А.С., Киселев А.В., Струков А.В., Скворцов М.С. Отчет о верификации программного средства «Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем» (АРБИТР, ПК АСМ СЗМА, базовая версия 1.0). Заключительная редакция с приложениями. СПб.: ОАО «СПИК СЗМА», 2007. — 1031 с.

5. АРБИТР, «Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА), базовая версия 1.0». Автор Можаев А.С. Правообладатель ОАО «СПИК СЗМА» // Свидетельство об официальной регистрации №2003611101. М.: РОСПАТЕНТ РФ, 2003 // Аттестационный паспорт №222 от 21 февраля 2007 г., выдан Советом по аттестации программных средств НТЦ ЯРБ Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ.

СВЕДЕНИЯ ОБ АВТОРАХ

Дурденко Владимир Андреевич. Профессор кафедры менеджмента. Доктор технических наук, доцент.
Воронежский институт инновационных систем.
E-mail: dva_viis@mail.ru
Россия, 394043, г. Воронеж, ул. Березовая роща, 54. Тел.(473) 2-354-898.

Рогожин Александр Александрович. Преподаватель кафедры технических систем безопасности.
Воронежский институт МВД России.
E-mail: raa_tsbs@list.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2-312-412.

Durdenko Vladimir Andreevich. Professor of the chair of Management. Doctor of technical sciences, assistant professor.
Voronezh Institute of Innovation Systems.
Work address: Russia, 394043, Voronezh, Berezovaya roscha Str., 54. Tel. (473) 2-354-898.

Rogozhin Alexander Alexandrovich. Lecturer of the chair of Technical Security Systems.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2-312-412.

Ключевые слова: интегрированная система безопасности; оценка надежности; общий логико-вероятностный метод, технология автоматизированного структурно-логического моделирования; схема функциональной целостности.

Key words: the integrated system of safety; the general logical and probabilistic method; technology of the automated structural and logical modeling; the scheme of functional integrity; estimation of reliability.

УДК 654.924; 621.38.019.3

А.В. Мишин,
кандидат технических наук, доцент,
Центральный филиал ФГБОУ ВПО «Российская академия правосудия»

С.А. Мишин,
кандидат технических наук, доцент,

МЕТОДИЧЕСКИЕ ПРИНЦИПЫ АППРОКСИМАЦИИ СЕПАРАБЕЛЬНЫХ ФУНКЦИЙ

METHODICAL PRINCIPLES OF APPROXIMATIONS SEPARABLE FUNCTION

Предложен конструктивный подход к решению задачи аппроксимации сепарабельных функций и методические принципы, позволяющие доступными средствами достичь требуемой надёжности её результатов. Изложение подкрепляется примером аппроксимации функции выбора максимального элемента.

The constructive approach to decision of the problem to approximations separable function and methodical principles, allowing available facility to reach required reliability her result, is offered. The interpretation is supported by example to approximations to functions of the choice of the maximum element.

Введение. В математическом анализе понятие функциональной зависимости между переменными *x* и *y* представляет математическую абстракцию реальных связей между величинами. Согласно определению функциональной зависимости предполагается, что каждому значению одной переменной соответствует определённое значение другой. Вместе с тем при обработке результатов наблюдений, экспериментов, измерений и т. д. приходится встречаться с таким положением, когда значениям зависимой переменной *y* ставятся в соответствие множества (векторы $\vec{x}$) значений переменной *x*, встречающиеся не одинаково часто и имеющие разную мощность. Функции подобного класса принято называть сепарабельными функциями. Так, перспективным подходом к реализации процедуры адаптации сетевых моделей целевых установок (СМЦУ) к деятельности конкретной организационной системы (ОС) является преобразование данной

модели к виду искусственной нейронной сети [2]. Однако такое преобразование требует решения ряда нетривиальных задач в частности, задачи аппроксимации для дизъюнктивных вершин функции выбора максимальной степени достижения подчинённых ЦУ при условии варьирования их количества (от двух до пяти), т.е., по сути, выбора максимального элемента вектора $\vec{x}$.

В связи с этим предлагаются постановка задачи аппроксимации сепарабельных функций, конструктивный подход к её решению и методические принципы, позволяющие доступными средствами достичь требуемой надёжности её результатов. Изложение подкрепляется примером аппроксимации функции выбора максимального элемента.

Постановка задачи и подход к её решению. Рассмотрим следующую задачу.

Пусть $\xi \in R^p$ и $\eta \in R^q$ — зависимые случайные векторы. Требуется по результатам наблюдений $(\vec{x}_1, ..., \vec{x}_n)$ за вектором ξ и $(y_1, \ \ldots, \ y_n)$ за вектором η сделать обоснованное заключение о виде (характере) зависимости η от ξ.

Теоретико-вероятностная формулировка подобного рода задач выглядит следующим образом [3]. Пусть $\rho(y', y'')$ — некоторая метрика в R^q. Требуется найти (борелевскую) функцию $\varphi\ (\cdot): R^p \to R^q$, для которой математическое ожидание $\mathrm{M}\,\rho(\eta, \varphi(\xi))$ принимает минимальное значение. В том случае, когда $\rho(y', y'') = \|y' - y''\|^2$ и $\|\cdot\|$ — евклидова норма в R^q, решение сформулированной задачи даётся функцией теоретической регрессии $y = \varphi_{\eta|\xi}(\vec{x})$, где

$$y = \varphi_{\eta|\xi}(\vec{x}) = \mathrm{M}[\eta | \xi = \vec{x}]. \qquad (1)$$

Решение задачи регрессии в форме (1) требует знания (или по крайней мере оценки) совместной функции распределения векторов ξ и η – информации, которой исследователь в большинстве случаев не располагает.

Примем следующие допущения и ограничения на решаемую задачу.

1. В качестве оценки теоретической функции регрессии $y = \varphi_{\eta|\xi}(\vec{x})$ выбирается функция $y = \varphi(\vec{x})$ из определённого, обладающего хорошими аппроксимирующими возможностями класса функций $\Phi = \{\varphi : R^p \to R^q\}$.

2. Функция $\varphi(\vec{x}) = \varphi(\vec{x}, \theta)$ однозначно определяется некоторым параметром $\theta \in \Theta$, где Θ – некоторая область в R^m (m фиксировано).

3. Возможен переход от функции $\varphi(\vec{x}, \theta)$ к функции $\varphi(x, \theta)$, где x – точечные оценки векторов $\vec{x} = (x_1 \quad ... \quad x_k \quad ...)$ и $x_k \in [0;1]$. Причём, функция $\varphi(x, \theta)$ зависит от θ линейно.

Получим следующую линейную модель регрессии:

$$y = \theta_0 \cdot \varphi_0(x) + \theta_1 \cdot \varphi_1(x) + ... + \theta_{m-1} \cdot \varphi_{m-1}(x), \qquad (2)$$

где $\varphi_i(x)$ – известные функции, определяющие план эксперимента, а m (порядок модели), x и параметр $\theta = (\theta_0, ..., \theta_{m-1})$ подлежат оценке на основе результатов наблюдений $(\vec{x}_1, ..., \vec{x}_n)$ и $(y_1, \ \ldots, \ y_n)$ с очевидным требованием $m < n$ (цель эксперимента).

4. Для получения точечных оценок неизвестных параметров (линейных) моделей используем метод наименьших квадратов (МНК), предполагающий в качестве то-

чечной оценки неизвестного параметра θ в (2) принятие оценки θ, исходя из предположения:

$$W(\theta) = \min_{\theta \in \Theta} \sum_{i=1}^{n} [\, y_i - \sum_{j=0}^{m-1} \varphi_j(\vec{x}_i)\,\theta_j \,]^2 = \sum_{i=1}^{n} [\, y_i - \sum_{j=0}^{m-1} \varphi_j(x_i)\,\theta_j \,]^2 . \quad (3)$$

Заметим, что в отличие от других методов точечного оценивания МНК на начальном этапе обработки результатов наблюдений не требует от исследователя знания априорной информации о виде распределений оцениваемых параметров [1]. Решение $\theta = (\theta_0, ..., \theta_{m-1})$ задачи (3) называется оценкой метода наименьших квадратов или МНК-оценкой параметра θ.

При такой постановке решаемой задачи конструктивным представляется следующий подход.

Шаг 1. Исходя из содержания аппроксимируемой функции, ввести правило замены векторов $\vec{x}$ их точечными x оценками.

Шаг 2. Установить порядок модели (первоначально $m = 1$, при очередном обращении – $m = m + 1$). По данным репрезентативной (но небольшого объёма) выборки подобрать подходящую аппроксимирующую функцию и соответствующие аппроксимирующие коэффициенты.

Шаг 3. Провести вычислительный эксперимент для получения эмпирического (статистического) распределения ошибок аппроксимации.

Шаг 4. Рассчитать числовые характеристики ошибки аппроксимации и оценить применимость полученных результатов для практики. При неудовлетворительных результатах аппроксимации вернуться к шагу 2, иначе – окончить данную процедуру.

Рассмотрим реализацию данного подхода на примере функции выбора максимального элемента.

Выбор аппроксимирующей функции. Вначале проанализируем возможность использования известных подходов к замене векторов $\vec{x}$ их точечными $\hat{x}$ оценками.

Задача отыскания максимального элемента не допускает мультипликативного подхода, позволяющего представить оценку $\hat{x}$ в виде произведения компонент вектора $\vec{x}$, т.к. она будет обращаться в нуль при нулевом значении любого компонента вектора $\vec{x}$. В связи с этим представляется разумным аддитивный подход, при котором оценка $\hat{x}$ представляется суммой значений x_k компонентов вектора $\vec{x}$:

$$x_i = \sum_{k=1}^{\tilde{N}} x_k , \quad (4)$$

где $\tilde{N}$ – количество компонент вектора $\vec{x}$.

Заметим, что априорное знание о частости проявления максимального значения у конкретного x_k компонента вектора $\vec{x}$ могло быть учтено предварительным умножением этих значений на соответствующие коэффициенты. В нашем случае оно отсутствует. Однако при накоплении опыта использования СМЦУ учёт этого знания представляется целесообразным.

Задачу (3) можно свести к решению системы уравнений

$$\frac{\partial W}{\partial \theta_0} = 0 , \ \frac{\partial W}{\partial \theta_1} = 0 , \ \ldots, \quad (5)$$

в которой число уравнений совпадает с числом неизвестных параметров.

Решить систему (5) в общем виде нельзя; для этого необходимо задаться конкретным видом функции $\varphi(x)$, но и в этом случае вычисление неизвестных параметров связано с трудоёмкими расчётами. В этой связи разумно воспользоваться доступными программными средствами, обладающими средствами аппроксимации функций методом наименьших квадратов. Например, средствами табличного процессора Microsoft Excel, реализующего приближения в виде прямой с уравнением $\tilde{y} = ax + b$ и линии с показательным (экспоненциальным) уравнением $\tilde{y} = b \cdot a^x$.

Выбор Microsoft Excel обусловлен двумя решающими факторами. Во-первых, его обширным распространением как неотъемлемого компонента Microsoft Office для операционной системы Windows. Приобретение же других лицензионных программных продуктов требует немалых денежных затрат, которые во многих случаях превышают стоимость компьютеров. Во-вторых, наличием навыков работы с данным приложением у широкого круга пользователей. Такие навыки целенаправленно прививаются обучаемым на курсах информатики не только в высших, но и в средних учебных заведениях.

Задачи, решённые с применением Microsoft Excel:

случайным образом сгенерирована последовательность (объёмом n = 100) наборов возможных значений $\vec{x}_i$ (степеней достижения подчинённых ЦУ) с учётом их $\tilde{N}$ количества ($\tilde{N} = \overline{2, 5}$);

для каждого i-го $(i = \overline{1, n})$ набора в качестве зависимой переменной выбрана $y_i = \max\limits_k \{x_1, ..., x_{\tilde{N}}\}$, а в качестве независимой переменной — оценка x, а также рассчитан коэффициент корреляции между ними;

для взаимного сравнения приближений по каждому из них рассчитана сумма квадратов $\sum\limits_{i=1}^{n} (y_i - \tilde{y}_i)^2$.

Напомним, что для расчёта коэффициентов a и b в Microsoft Excel можно воспользоваться средством «Анализ данных» или в соответствующие ячейки электронной таблицы при приближении в виде прямой ввести следующие формулы:

$$= \text{ИНДЕКС(ЛИНЕЙН}(y_1 : y_n ; x_1 : x_n);1)$$

$$= \text{ИНДЕКС(ЛИНЕЙН } y_1 : y_n ; x_1 : x_n);2),$$

при приближении в виде линии с показательным уравнением:

$$=\text{ИНДЕКС(ЛГРФПРИБЛ}(y_1 : y_n ; x_1 : x_n);1)$$

$$=\text{ИНДЕКС(ЛГРФПРИБЛ}(y_1 : y_n ; x_1 : x_n);2),$$

где $x_1 : x_n$ – блок ячеек с оценками $\hat{x}$; $y_1 : y_n$ – блок ячеек значений зависимой переменной. А для расчёта коэффициента корреляции между этими величинами ввести формулу

$$=\text{КОРРЕЛ}(x_1 : x_n ; y_1 : y_n).$$

Результаты данного этапа (округление до 6 знака после запятой) представлены в табл. 1.

Таблица 1

Результаты аппроксимации средствами Microsoft Excel

$\tilde{N}$	Коэффиц. корреляции	$\tilde{y} = ax + b$		$\tilde{y} = b \cdot a^x$		Сумма квадратов	
		a	b	a	b	линейн.	показат.
2	0,863868	0,5	0,165	5,939668	0,248607	1,4025	2,562313
3	0,751297	0,284661	0,353156	3,315875	0,414787	1,271814	1,514117
4	0,830034	0,219145	0,340072	3,415069	0,407739	0,908245	1,133767
5	0,702940	0,109567	0,598334	1,884159	0,111259	0,455086	1,656895

Анализ полученных данных (табл. 1) позволил сделать два вывода.

Во-первых, наиболее подходящим для аппроксимации является линейное (в виде прямой) приближение.

Во-вторых, для выбора аппроксимирующих коэффициентов необходим непосредственный учёт количества $\tilde{N}$, т.е. функций $a = a(\tilde{N})$ и $b = b(\tilde{N})$:

$$a = \begin{cases} 0{,}5, & \text{если } \tilde{N} = 2; \\ 0{,}2846608, & \text{если } \tilde{N} = 3; \\ 0{,}2191454, & \text{если } \tilde{N} = 4; \\ 0{,}1095672, & \text{если } \tilde{N} = 5. \end{cases} \tag{6}$$

$$b = \begin{cases} 0{,}165, & \text{если } \tilde{N} = 2; \\ 0{,}3531563, & \text{если } \tilde{N} = 3; \\ 0{,}3400716, & \text{если } \tilde{N} = 4; \\ 0{,}5983337, & \text{если } \tilde{N} = 5. \end{cases} \tag{7}$$

Проведение и обработка результатов эксперимента. Для получения эмпирического (статистического) распределения ошибок аппроксимации проведен вычислительный эксперимент, укрупнённая схема которого показана на рис. 1.

В ходе вычислительного эксперимента решались следующие задачи:

1) моделирование выборки возможных наборов (векторов $\vec{x}$) — $\{x_k \mid \forall_{k,\,\tilde{N}} : x_k \in (0.1, 0.2, ..., 1), (k = 1, ..., \tilde{N}), \tilde{N} = (\overline{2,\ 5})\}$. Поскольку количество r_k разных значений для каждого x_i равно 10, то по комбинаторным правилам умножения и сложения общее количество M возможных наборов (объём выборки) составило

$$M = r_1 r_2 + r_1 r_2 r_3 + r_1 r_2 r_3 r_4 + r_1 r_2 r_3 r_4 r_5 = r_1 r_2 (1 + r_3 (1 + r_4 (1 + r_5))) = 111100.$$

2) расчёт для каждого i-го набора значений переменных $x_i = \sum_{k=1}^{\tilde{N}} x_k$ и $y_i = \max_k \{x_1, ..., x_{\tilde{N}}\}$, а также ошибки Δ_i аппроксимации

$$\Delta_i = y_i - [a(\tilde{N}) \cdot x_i + b(\tilde{N})], \tag{8}$$

где значения коэффициента $a(\tilde{N})$ определяются из (6), коэффициента $b(\tilde{N})$ — из (7);

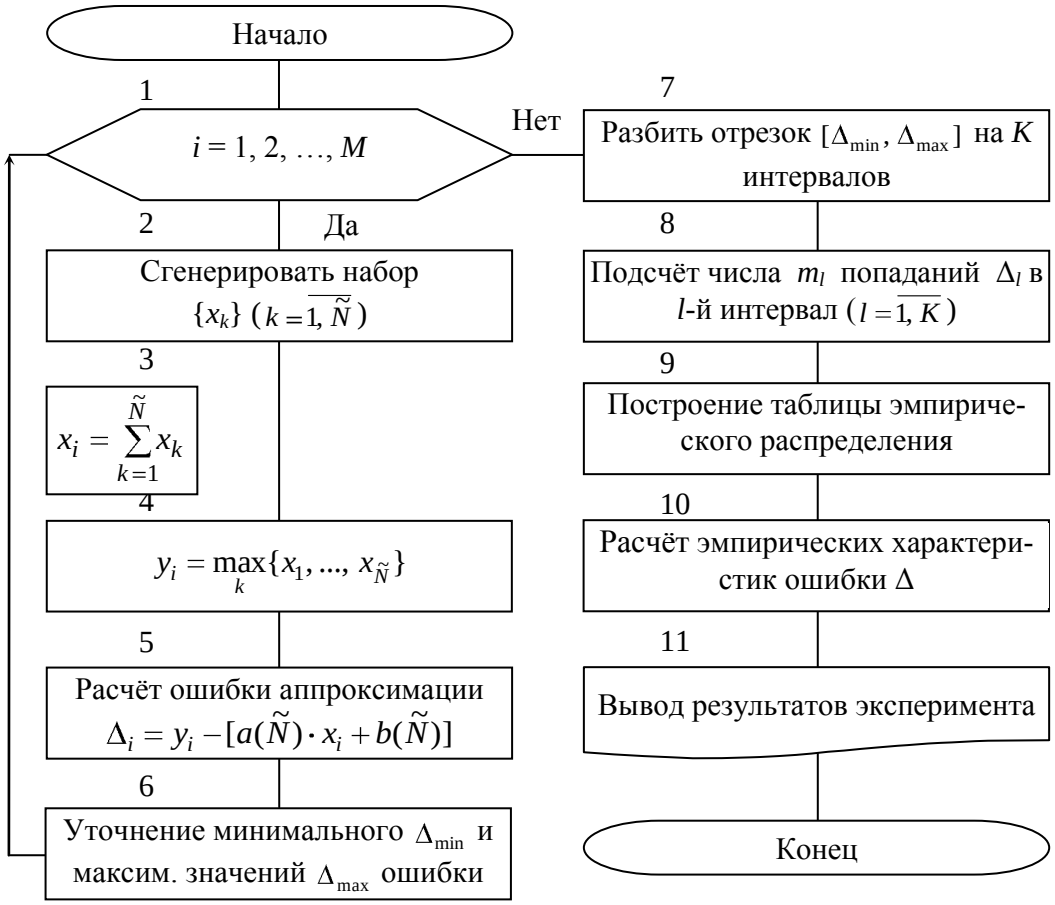


Рис. 1. Укрупнённая схема вычислительного эксперимента

3) определение минимального $\Delta_{\min}$ и максимального $\Delta_{\max}$ значений наблюдаемых ошибок аппроксимации;

4) обработка результатов наблюдения, включающая построение интервальной таблицы эмпирического распределения ошибок аппроксимации и расчёт числовых характеристик: эмпирического среднего $\bar{x}$, выборочной дисперсии S^2 и выборочного среднеквадратичного отклонения σ.

Большой объём выборки (M = 111100) осложняет (в силу трудоёмкости заполнения электронной таблицы) использование Microsoft Excel и обусловил необходимость моделирования эксперимента на одном из языков программирования. В качестве такового (для реализации шагов 1—8, рис. 1) был использован Microsoft Visual Basic.

Экспериментом установлено, что разброс ошибок аппроксимации Δ_i $(i = \overline{1, M})$ составил от – 0,553 до 0,594. Данный диапазон был разбит на 7 равных (длиной ΔI) интервалов, и для каждого из них рассчитано его среднее X_l значение. Результаты подсчёта числа m_l попаданий в l-й $(l = \overline{1, 7})$ интервал представлены в третьей строке табл. 2.

Таблица 2

Таблица эмпирического распределения ошибок аппроксимации

Интервалы	(– 0,55; – 0,39)	(– 0,39; – 0,23)	(– 0,23; – 0,06)	(– 0,06; 0,1)	(0,1; 0,27)	(0,27; 0,43)	(0,43; 0,594)
X_l	– 0,4712	– 0,3073	– 0,1434	0,0205	0,1844	0,3483	0,5122
m_l	239	4720	26081	62119	16310	1501	130
$\tilde{p}_l$	0,00215	0,0425	0,2348	0,5591	0,1468	0,0135	0,0012
$\tilde{f}_l$	0,01313	0,2592	1,4323	3,4114	0,8957	0,0824	0,0071
$\tilde{F}_l$	0,00215	0,0446	0,2794	0,8385	0,9853	0,9988	1

Последующие шаги (9—11, рис. 1) реализовывались средствами Microsoft Excel. В частности, расчёт значений показателей таблицы эмпирического (статистического) распределения ошибок аппроксимации (табл. 2) осуществлялся по следующим известным формулам.

Относительная частота $\tilde{p}_l$ попадания Δ_i в l-й интервал:

$$\tilde{p}_l = \frac{m_l}{M}. \qquad (9)$$

Значения плотности $\tilde{f}_l$ относительной частоты попадания Δ_i в l-й интервал:

$$\tilde{f}_l = \frac{\tilde{p}_l}{\Delta I}. \qquad (10)$$

Значения накопленной частоты $\tilde{F}_l$ (эмпирической функции распределения) для l-го интервала:

$$\tilde{F}_l = \sum_{s=1}^{l} \tilde{p}_s. \qquad (11)$$

Графики эмпирической плотности распределения (полигон) и эмпирической функции распределения (кумулята) ошибок аппроксимации представлены на рис. 2 и рис. 3, соответственно. Характер полигона выборки (рис. 2) позволяет утверждать, что ошибки аппроксимации распределены по нормальному закону.

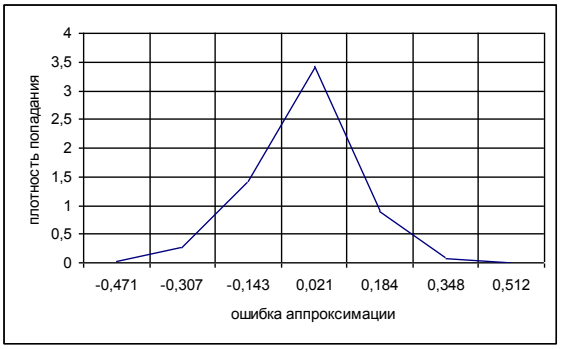


Рис. 2

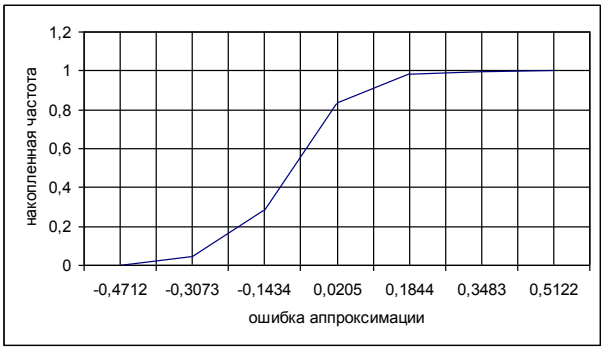


Рис. 3

Оценка параметров эмпирического распределения. Расчёт числовых характеристик ошибки аппроксимации производился по следующим известным формулам.

Эмпирическое среднее $\bar{x}$:

$$\bar{x} = \sum_{l=1}^{K} x_l \cdot \tilde{p}_l \ . \tag{12}$$

Эмпирическая (выборочная) дисперсия S^2:

$$S^2 = \sum_{l=1}^{K} x_l^2 \cdot \tilde{p}_l - (\bar{x})^2 . \tag{13}$$

Эмпирическое (выборочное) среднеквадратичное отклонение σ:

$$\sigma = \sqrt{S^2} \ . \tag{14}$$

В результате получены: $\bar{x} = -0{,}00386,\ S^2 = 0{,}016475,\ \sigma = 0{,}128353.$

На завершающем этапе аппроксимации полученные результаты оценивались с позиции возможности их практического применения.

Заметим, что выборочная совокупность представляет лишь часть генеральной совокупности. Вполне естественно, что выборочные характеристики не будут точно совпадать с соответствующими характеристиками генеральной совокупности. Для уточнения такого несоответствия статистика предлагает широко развитый математический аппарат интервальной оценки параметров эмпирического распределения [1, 3].

При последующем рассмотрении правил построения доверительного интервала ограничимся случаем, когда случайная величина имеет нормальное распределение с параметрами m и σ и оценивается только математическое ожидание.

Доверительный интервал для математического ожидания m нормального распределения с уровнем доверия (доверительной вероятностью) α при известном среднеквадратичном отклонении σ определяется из соотношения:

$$\bar{x} - k_\alpha \cdot \frac{\sigma}{\sqrt{n}} < m < \bar{x} + k_\alpha \cdot \frac{\sigma}{\sqrt{n}} , \tag{15}$$

где k_α — аргумент функции Лапласа (интеграла вероятностей) $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt$,

для которого $\Phi(k_\alpha) = \alpha/2$ (определяется из таблицы, представленной в справочниках по математической статистике, например, в [1, с. 578]).

Отметим, что соотношением (15) можно пользоваться всегда, когда среднеквадратичное отклонение известно или установлено по выборке достаточно большого объёма ($n \geq 50$).

Зададимся уровнем доверия α = 0,95. Из таблицы функции Лапласа находим $k_\alpha \approx 1{,}96$. Подставив полученные данные в (15), получим:

$$\bar{x} - 1{,}96 \cdot \frac{0{,}128353}{\sqrt{111100}} < m < \bar{x} + 1{,}96 \cdot \frac{0{,}128353}{\sqrt{111100}} \Rightarrow m \in (-0{,}00461; -0{,}00311).$$

Для нашего случая — задачи аппроксимации для дизъюнктивных вершин функции выбора максимальной степени достижения подчинённых ЦУ — результат аппроксимации является вполне приемлемым: расхождение в доли процента в СМЦУ не окажет существенного влияния на оценку эффективности деятельности ОС.

Заключение. Предложенный подход применим к решению задачи аппроксимации сепарабельных функций и позволяет доступными средствами достичь требуемой надёжности её результатов. Интерес к функции выбора максимального элемента обусловлен областью научных интересов авторов — выработкой механизмов поиска решений на сетевых моделях. Вместе с тем, очевидно, что подобные функции затрагивают более широкие области практического применения.

ЛИТЕРАТУРА

1. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). — М.: Наука, 1973. — 832 с.

2. Мишин А.В., Мишин С.А. Приведение модели целей организационной системы к структуре нейронной сети // Охрана, безопасность и связь – 2012: материалы международ. научно-практич. конф. Часть 2. — Воронеж: Воронежский институт МВД России, 2012. — С. 43—46.

3. Справочник по теории вероятностей и математической статистике / В.С. Королюк [и др.]. — М.: Наука. Главная редакция физико-математической литературы, 1985. — 640 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Александр Владимирович. Заведующий кафедрой правовой информатики, информационного права и естественнонаучных дисциплин. Кандидат технических наук, доцент.

Центральный филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российская академия правосудия» (г. Воронеж).

E-mail: odpvo@mail.ru

Россия, 394006, г. Воронеж, ул. 20-летия Октября, 95. Тел. (473) 271-54-15.

Мишин Сергей Александрович. Старший преподаватель кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: samishin@bk.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 262-32-78.

Mishin Alexander Vladimirovich. Chief of the chair of the legal informatics, information law and natural-science disciplines. Candidate of sciences (technics), assistant professor.

The Central branch of the federal state budgetary educational institution of the professional higher education "Russian Academy of Justice" (Voronezh).

Work address: Russia, 394006, Voronezh, 20 Years of October str., 95. Tel. (473) 271-54-15.

Mishin Sergey Alexandrovich. Senior lecturer of the chair of automated information systems of the Law Enforcement Agencies. Candidate of sciences (technics), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 262-32-78.

Ключевые слова: аппроксимация; функция, максимальный элемент; модель регрессии; метод наименьших квадратов.

Key words: approximation; function; maximum element; model to regressions; least square method.

УДК 681.3