АЛГОРИТМИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПОДРАЗДЕЛЕНИЯ ГПС МЧС РОССИИ

В.И. Антюхов, кандидат технических наук, профессор;
О.В. Кравчук.
Санкт-Петербургский университет ГПС МЧС России

Предложены алгоритм функционирования системы управления рисками информационно-вычислительной сети подразделения ГПС МЧС России, разработанный с использованием графического, агрегативного и теоретико-множественного способов описания сложных систем и алгоритм управления информационными рисками.

Ключевые слова: алгоритм, риск, управление информационным риском, система управления

ALGORITHMIZATION OF THE RISK MANAGEMENT PROCESS OF INFORMATION-COMPUTER NETWORK OF DEPARTMENT OF STATE FIRE SERVICE OF EMERCOM OF RUSSIA

V.I. Antyukhov; O.V. Kravchuk.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The algorithm of the system of risk management of information-computer network of department of State fire service of EMERCOM of Russia, developed using the graphical, aggregate and set-theoretic methods of describing complex systems and an algorithm for information risk management are proposed.

Keywords: algorithm, risk, management risk, system of management

Анализ литературы по вопросам описания сложных систем и управления информационными рисками (ИР) позволяет сделать вывод, что зависимость успешной деятельности подразделений ГПС МЧС России от автоматизированных систем обработки информации и принятия решений объективно приводит к наступлению в информационно-вычислительной сети (ИВС) случайных событий – информационных рисков [1–3]. В связи с тем, что игнорирование наличия ИР в подразделении может привести к появлению в его ИВС негативных событий, необходимо научиться управлять ИР, с целью снижения критичности последствий, которые могут наступить в сети в результате реализации ИР.

Реализовать процесс управления ИР невозможно без соответствующей системы управления информационными рисками (СУИР), разработка и внедрение которой в подразделения ГПС МЧС России позволит повысить уровень информационной безопасности (ИБ) ИВС подразделений.

Анализ текущего состояния информационной безопасности ИВС подразделений ГПС МЧС России и на ближайшую перспективу позволяет предложить СУИР, состоящую из шести подсистем [4–6]:

1. Подсистема разработки концептуальной модели СУИР (подсистема 1), задачей которой является обеспечение разработчика (лица принимающего решение (ЛПР) СУИР на начальном этапе работ необходимым и достаточным набором исходных данных для установления контекста управления информационными рисками.

2. Подсистема выявления угроз, их фиксации и журналирования (подсистема 2), предназначенная для разработки совокупности сценариев развития событий в ИВС подразделения ГПС МЧС России при воздействии на нее возможных дестабилизирующих факторов, фиксации и документирования сценариев в СУИР. Для каждого сценария предполагается получение параметров ИР (в крайнем случае, его качественной оценки).

3. Подсистема выбора и принятия решения, относительно управляющих воздействий (подсистема 3), обеспечивающая выбор способа обработки ИР (снижение риска, сохранение риска, избегание риска, перенос риска) в соответствии с его уровнем. На основе выбранного способа и данных, полученных в результате функционирования подсистем 1 и 2, должна осуществляться выработка множества альтернатив управляющих воздействий и их выбор ЛПР.

4. Подсистема реализации управляющих воздействий (подсистема 4), осуществляющая доведение решения до исполнителей, а также внедрение в процесс функционирования подразделения ГПС МЧС России, в частности ИВС подразделения, выбранных средств и методов управления.

5. Подсистема оценивания эффективности управляющих воздействий (подсистема 5) относительно выявленных угроз в соответствии со сформированными критериями эффективности.

6. Подсистема обеспечения непрерывности процесса управления ИР (подсистема 6), задачами которой являются:

– проведение корректирующих мероприятий относительно структуры СУИР и принимаемых в процессе ее функционирования решений;

– непрерывный анализ и аудит принимаемых решений и результатов функционирования СУИР со стороны ЛПР и руководства подразделения ГПС МЧС России с целью идентификации любых изменений.

Цикличность процесса управления рисками типовой ИВС подразделения ГПС МЧС России предполагает возвращение к первой подсистеме управления для корректировки концептуальной модели СУИР по результатам предыдущей итерации.

Можно предположить, что, так как СУИР является системой с последействием, то алгоритм функционирования подсистемы разработки концептуальной модели СУИР будет «зависеть» от алгоритмов функционирования «нижестоящих» подсистем и для его актуализации необходимо уметь описывать процесс функционирования «нижестоящих» подсистем.

Для реализации процесса управления ИР с использованием алгоритмов функционирования СУИР предлагается способ описания процесса функционирования элементов и подсистем СУИР на концептуальном (частично функциональном уровне), а также формальном уровнях с использованием теории агрегатов [7, 8].

Агрегативное описание процесса управления ИР с использованием СУИР представляется возможным вследствие своей компактности, наглядности, быстродействия, единства процедур описания и удобства реализации на ЭВМ.

Алгоритм функционирования любого элемента/подсистемы СУИР можно представить последовательностью действий, выполняемых агрегатами (элементами/подсистемами). Каждая группа элементарных операций алгоритма представляется операторами, отражающими его логическую структуру. Такими операторами являются:

– оператор N – специфический оператор, обозначающий окончание вычислений;

– оператор A – арифметический оператор – совокупность операций, реализующих какое-либо соотношение или систему соотношений между величинами;

– оператор L – логический оператор – предназначен для проверки справедливости заданных условий и выработки признаков, обозначающих результат проверки;

– оператор S – оператор формирования реализаций случайных процессов, вводимый для имитации действия различных случайных факторов, сопровождающих исследуемый процесс;

– оператор J – оператор формирования реализаций неслучайных величин, вводимый при моделировании процесса функционирования элемента/подсистемы СУИР для реализации различных констант и не случайных функций времени;

– оператор C – служебный оператор моделирующего алгоритма, вводимый для подсчета количества различных объектов, обладающих заданными свойствами.

Описание операторов алгоритма функционирования элементов/подсистем СУИР представлено в таблице [6–8].

Таблица. **Описание операторов алгоритма функционирования элементов/подсистем СУИР**

Наименование оператора	Назначение оператора	Наименование подоператора	Назначение подоператора
N	Специальный оператор, означающий начало/конец вычислений	N_1	Начало функционирования агрегата/подсистемы
		N_{43}	Окончание функционирования агрегата/подсистемы. Выдача результатов
A	Описание действий, связанных с вычислениями	A_5/ A_6	Внесение значений начала ($t_{h\varphi n}$) и окончания ($t_{h\varphi z}$) функционирования агрегата/подсистемы в память ЭВМ
		A_{10}/A_{15}	Внесение значений моментов поступления управляющего (τ_e) и входного (t_u) сигналов в память ЭВМ
		A_{20}	Определение ближайшего момента ($t_{вых}$) выдачи агрегатом/подсистемой выходного сигнала, содержащего отрывок выходного сообщения $(t, g_N)_T$
		A_{38}	Фиксация результатов, полученных при функционировании рассматриваемого агрегата/подсистемы
		A_{42}	Обработка результатов функционирования рассматриваемого агрегата/подсистемы
J	Оператор формирования неслучайных процессов	J_4	Формирование значений характеристик агрегата/подсистемы (Zn_γ)
		J_{19}	Формирование оператора ($U_{t_{h\varphi n}}$) для определения состояния агрегата/подсистемы в промежутках между особыми состояниями
		J_{22}	Определение состояния агрегата/подсистемы в момент $t_{вых}$
		J_{23}	Формирование выходного сигнала ($g_{h\nu}$), содержащего отрывок выходного сообщения
		J_{24}	Формирование состояния агрегата/подсистемы ($z(t_{вых}+0)$) после выдачи выходного сигнала
		J_{27}	Определение состояния агрегата/подсистемы ($z(t_{вх})$) в момент $t_{вх}$
		J_{29}/J_{32}	Формирование управляющего и входного сигналов соответственно, содержащих отрывки управляющего и входного сообщений ($(\tau, y_\Omega)_T$, $(t, x_\psi)_T$)
		J_{30}/J_{33}	Определение состояний агрегата/подсистемы ($z(\tau_e+0)$/$z(t_u+0)$) после поступления управляющего/входного сигнала соответственно
		J_{36}	Определение состояния агрегата/подсистемы $z(t_{h\varphi z})$ в момент окончания моделирования функционирования агрегата (активной фазы агрегата)
		J_{37}	Формирование предыстории ($(\tau_{B_u}, z_\omega)_{\tau_e}$)/($(t_{B_u}, z_\omega)_{t_u}$)) функционирования агрегата/подсистемы

		J_{41}	Переход к моделированию очередной реализации алгоритма функционирования агрегата/подсистемы
S	Оператор формирования случайных процессов	S_2, S_3	Формирование моментов начала ($t_{h\varphi n}$) и окончания $t_{h\varphi z}$ активной фазы этапа функционирования агрегата/подсистемы соответственно
		S_7	Формирование очередного момента (τ_e) поступления в агрегат/подсистему управляющего сигнала, содержащего отрывок управляющего сообщения $(\tau, y_Q)_T$
		S_9/ S_{16}	Подстановка вместо τ_e/t_u соответственно величины $t_{h\varphi z}$
		S_{13}	Формирование очередного момента t_u поступления в агрегат/подсистему входного сообщения $(t, x_\psi)_T$
		S_{17}/ S_{18}	Формирование признака $\gamma=0/\gamma=1$ – «ближайшим сообщением будет управляющее $t_{вх}=\tau_e$ /входное сообщение $t_{вх}=t_u$» соответственно
		S_{35}	Подстановка вместо $t_{h\varphi n}$ момента t_{oc} – последнего особого состояния
L	Логический оператор, осуществля-ющий проверку справедливости заданных условий и выработку признаков, обозначающих результат проверки	L_8	Проверка условия $\tau_e \leqq t_{h\varphi z}$
		L_{11}	Проверка условия e> 1
		L_{12}	Проверка условия условия $t_u<\tau_e$, где t_u – момент поступления входного сообщения $(t, x_\psi)_T$
		L_{14}	Проверка условия $t_u<t_{h\varphi z}$
		L_{21}	Проверка условия $t_{вых} \leq t_{вх}$, где $t_{вх}=\min(\tau_e, t_u)$
		L_{25}/ L_{31}/ L_{34}	Проверка принадлежности состояний $z(t_{вых}+0)/z(\tau_e+0)/z(t_u+0)$ соответственно подмножеству Z_y
		L_{26}	Проверка условия $t_{вх}<t_{h\varphi z}$
		L_{28}	Проверка условия $\gamma> 0$
		L_{40}	Проверка N<N*, где N* – заданное количество реализаций
C	Счетчик	C_{39}	Счетчик количества реализаций N

С учетом схемы описания операторов элементов/подсистем СУИР ее операторная схема будет иметь вид: N_1, S_2, S_3, J_4, A_5, A_6, $^{31,\ 41}S_7$, $L_8^{\uparrow 10}$, S_9^{11} , $^{8}A_{10}$, $^{9}L_{11\downarrow 13}$, $^{15,16}L_{12\downarrow 17}^{\uparrow 18}$, $^{11,34}S_{13}$, , $L_{14\downarrow 16}$, A_{15}^{12} , $^{14}S_{16}^{12}$, $^{12}S_{17}^{35}$, $^{12}S_{18}^{35}$, $^{35}J_{19}$, A_{20}, $L_{21\downarrow 26}$, J_{22}, $^{25,31,34}J_{23}$, J_{24}, $L_{25\downarrow 35}^{\uparrow 23}$, $^{21}L_{26\downarrow 36}$, J_{27}, $L_{28}^{\uparrow 32}$, J_{29}, J_{30}, $L_{31\downarrow 7}^{\uparrow 23}$, $^{28}J_{32}$, J_{33}, $L_{34\downarrow 13}^{\uparrow 23}$, $^{17,\ 18,\ 25}S_{35}^{19}$, $^{26}J_{36}$, J_{37}, A_{38}, C_{39}, $L_{40\downarrow 42}$, J_{41}^{7} , $^{40}A_{42}$, N_{43},

где, например,

– S_9^{11} означает, что от оператора № 9 передается управление оператору № 11;

– $L_{12\downarrow 17}^{\uparrow 18}$ означает, что от логического оператора № 12 управление следует передать оператору № 18, в случае выполнения проверяемого условия или оператору № 17, в случае его невыполнения;

– $^{8}A_{10}$ означает, что оператору № 10 передано управление от оператора № 8.

Усовершенствованная операторная схема алгоритма функционирования позволяет описать процесс функционирования любого элемента и подсистемы СУИР и разработать модель процесса их функционирования на ЭВМ.

Таким образом, результаты функционирования подсистем 2, 3, 4, 5, 6 позволят осуществить совершенствование первой подсистемы – подсистемы разработки концептуальной модели СУИР подразделения ГПС МЧС России на основе полученных ранее данных.

Управление ИР осуществляется в интересах сотрудников, отвечающих за защиту информации и обеспечения безопасности спасательных работ, в частности сотрудников подразделений, отвечающих за организацию и устойчивую работу систем связи, технических комплексов и средств автоматизации и оповещения подразделений МЧС России, а также сотрудников оперативно-аналитических, информационно-аналитических отделов, отделов по работе с информационными ресурсами и подготовки информации. Из числа сотрудников указанных подразделений формируется рабочая группа, отвечающая всем требованиям формирования экспертных групп, и назначается ЛПР. Сформированная группа осуществляет управление ИР в соответствии с алгоритмом, содержащим следующие блоки, соответствующие подсистемам концептуальной схемы алгоритма процесса управления рисками типовой информационно-вычислительной сети подразделения ГПС МЧС России:

– блок 1 (1 элемент алгоритма) – начало работы;

– блок 2 (1–13) – разработка концептуальной модели СУИР;

– блок 3 (1–19) – выявление угроз ИВС, их фиксации и журналирования;

– блок 4 (20–23) – выработка и принятие решения относительно управляющих воздействий;

– блок 5 (24) – реализация принятых решений;

– блок 6 (25–27) – оценка эффективности принятых решений;

– блок 7 (28–30) – обеспечение непрерывности процесса управления ИР.

– блок 8 (31) – окончание работы.

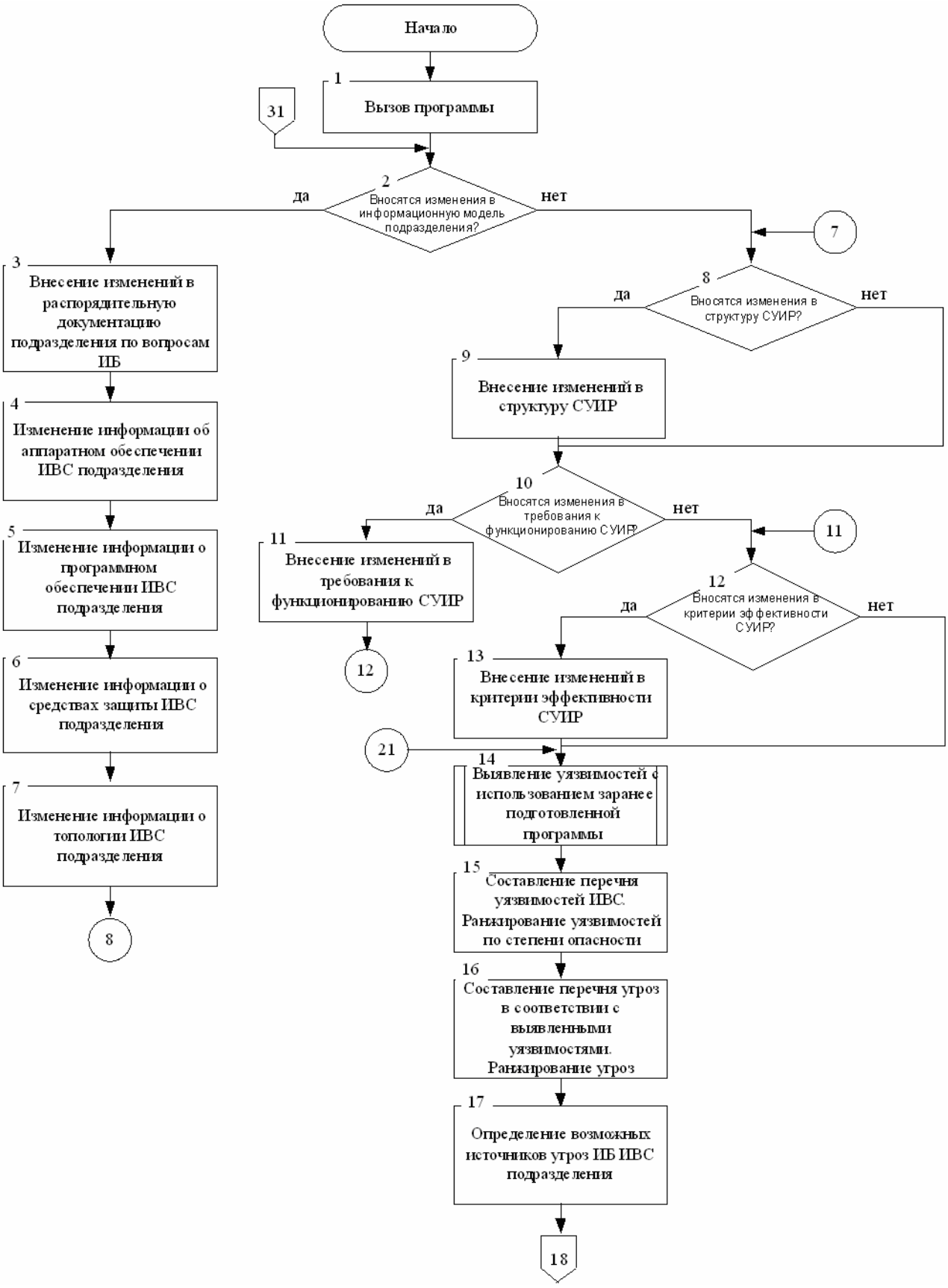
Блок-схема рассматриваемого алгоритма представлена на рисунке. Блок-схема алгоритма является основой для разработки методики управления ИР и автоматизации процесса управления рисками ИВС подразделений ГПС МЧС России с целью дальнейшего внедрения в практическую деятельность подразделений.

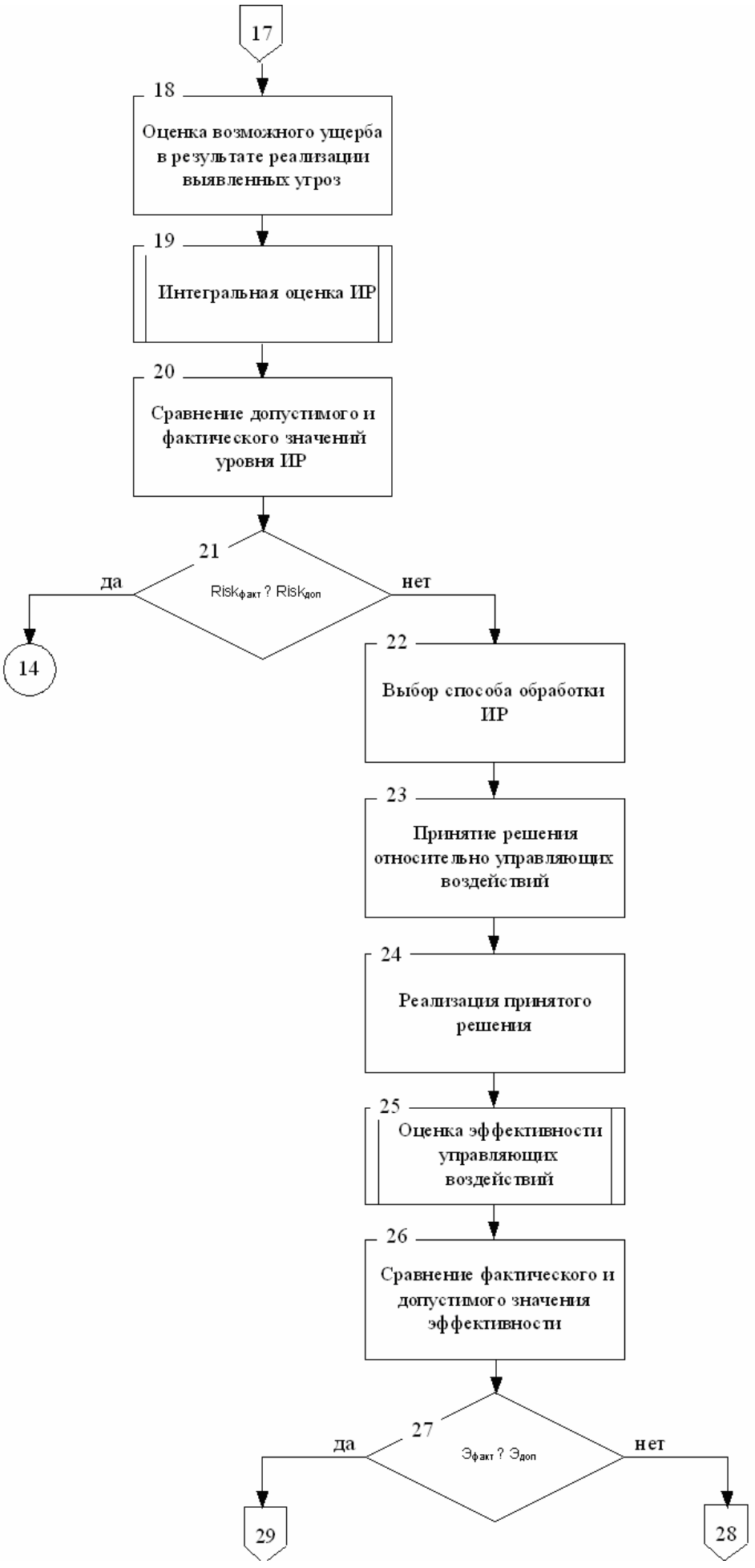
По итогам первой итерации рабочая группа во главе с ЛПР имеют следующие сведения: перечень уязвимостей ИВС подразделения; перечень угроз ИВС подразделения; перечень сценариев развития событий, содержащий различные комбинации уязвимостей, угроз и последствий их реализации; значение уровня ИР подразделения; рекомендации по выбору способа обработки ИР и соответствующий комплекс управляющих воздействий по обработке ИР, значение эффективности принятого решения относительно управляющих воздействий и значение эффективности разработанной СУИР. По значению показателя эффективности СУИР ЛПР совместно с экспертной группой принимают решение об изменении структуры СУИР. Если СУИР не требует изменений, осуществляется вторая итерация управления.

Выводы:

– в статье представлен усовершенствованный алгоритм функционирования элементов/подсистем СУИР с использованием графического, агрегативного и теоретико-множественного способов описания сложных систем;

– разработан алгоритм процесса управления рисками, возникающими в ИВС подразделений ГПС МЧС России в виде блок-схемы, что позволит в дальнейшем разработать методику управления ИР и автоматизировать процесс управления рисками, возникающими в ИВС, и внедрить в практическую деятельность подразделений.


Начало
1
Вызов программы
31
2
Вносятся изменения в информационную модель подразделения?
да
нет
3
Внесение изменений в распорядительную документацию подразделения по вопросам ИБ
4
Изменение информации об аппаратном обеспечении ИВС подразделения
5
Изменение информации о программном обеспечении ИВС подразделения
6
Изменение информации о средствах защиты ИВС подразделения
7
Изменение информации о топологии ИВС подразделения
8
7
8
Вносятся изменения в структуру СУИР?
да
нет
9
Внесение изменений в структуру СУИР
10
Вносятся изменения в требования к функционированию СУИР?
да
нет
11
Внесение изменений в требования к функционированию СУИР
12
11
12
Вносятся изменения в критерии эффективности СУИР?
да
нет
13
Внесение изменений в критерии эффективности СУИР
21
14
Выявление уязвимостей с использованием заранее подготовленной программы
15
Составление перечня уязвимостей ИВС. Ранжирование уязвимостей по степени опасности
16
Составление перечня угроз в соответствии с выявленными уязвимостями. Ранжирование угроз
17
Определение возможных источников угроз ИБ ИВС подразделения
18


17
18
Оценка возможного ущерба в результате реализации выявленных угроз
19
Интегральная оценка ИР
20
Сравнение допустимого и фактического значений уровня ИР
21
RiskФакт ? RiskДоп
да
нет
14
22
Выбор способа обработки ИР
23
Принятие решения относительно управляющих воздействий
24
Реализация принятого решения
25
Оценка эффективности управляющих воздействий
26
Сравнение фактического и допустимого значения эффективности
27
ЭФакт ? ЭДоп
да
нет
29
28

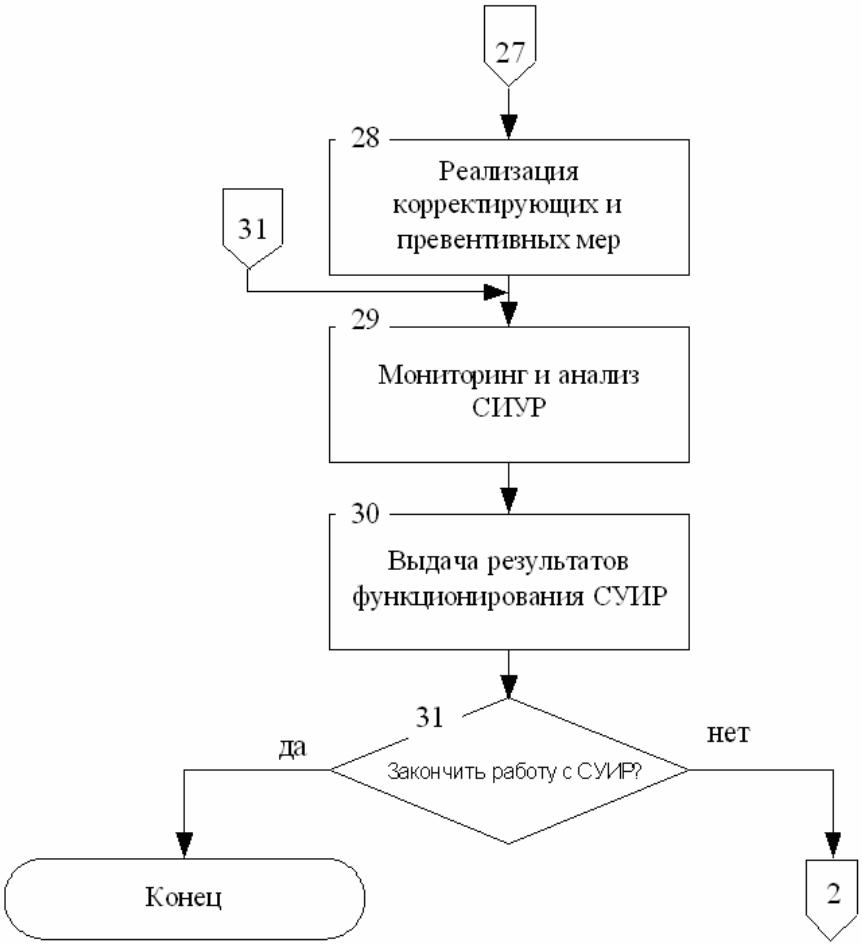


Рис. **Блок-схема алгоритма процесса управления рисками типовой ИВС подразделения ГПС МЧС России**

Литература

1. Варфоломеев А.А. Управление информационными рисками: учеб. пособие. М.: РУДН, 2008. 158 с.

2. Чернова Г.В., Кудрявцев А.А. Управление рисками: учеб. пособие. М.: ТК Велби; Изд-во Проспект, 2003. 160 с.

3. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010.

4. Антюхов В.И., Кравчук О.В. Методика описания системы управления рисками типовой информационно-вычислительной сети подразделения ГПС МЧС России // Проблемы управления рисками в техносфере. 2014. № 2 (30). С. 41–49.

5. Антюхов В.И., Кравчук О.В. Автоматизированное управление рисками в типовой информационно-вычислительной сети подразделения ГПС МЧС России // Природные и техногенные риски (физико-математические и прикладные аспекты). 2013. № 4 (8). С. 51–58.

6. Антюхов В.И., Кравчук О.В. Формальная модель системы управления рисками типовой информационно-вычислительной сети подразделения ГПС МЧС России // Проблемы управления рисками в техносфере. 2014. № 3 (31). С. 37–47.

7. Острейковский В.А. Теория систем: учеб. М.: Высш. шк., 1997. 239 с.

8. Бусленко Н.П. Моделирование сложных систем. М.: Гл. ред. физ.-матем. лит-ры изд-ва «Наука», 1978.