Published in the Slovak Republic
European Journal of Computer Science
Has been issued since 2015.
E-ISSN 2500-1035
2018, 4(1): 17-26

DOI: 10.13187/ejcs.2018.1.17
www.ejournal39.com

Structure of the General Algorithm of Dynamic Management of Activity Service Physical Protection Information in ASDP

Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a], Andrey S. Kopyrin [a], Margarita A. Kardashyan [a], Valentina V. Kopyeva [a]

[a] Sochi State University, Russian Federation

Abstract

The work is devoted to the development of a general algorithm for the dynamic management of the activity of the service of the physical protection of information in the ASDP. For the effective implementation of the activities of the service of protection offered a universal flowchart of the psycho-heuristic program for the formation of directories of malicious actions, protection tasks and remedies. Regular use of the psycho-heuristic program in the service of protection provides the following: 1) training of the service of protection; 2) actualization of existing directories: malicious actions, tasks and remedies.

Keywords: physical protection of information, psycho-heuristic program, probability of malicious actions, means of protection, information protection service.

1. Введение

К настоящему времени концепция ОДУ защитой информации в АСОД разработана достаточно полно и стройно. Основные положения её изложены в (Герасименко, Милославская, 1997; Герасименко, Малюк, 1997; Simavoryan et al., 2018; Пономаренко, 2010; Аверченков, Рытов, 2016). Основу развиваемых здесь положений составляет утверждение, что управление службой охраны АСОД является частным случаем управления защитой информации в АСОД. Поэтому структура и содержание процессов управления деятельностью охранной службы защиты должны определяться на основе общих концепций управления в больших организационно-технологических системах. Структура общего алгоритма динамического управления деятельностью службы физической защиты информации приводится на Рисунке 1. Следует подчеркнуть, что в основе алгоритма лежит понятие полноты функций защиты информации с точки зрения охранных функций, вытекающих из общих положений, сформулированных в работе (Simavoryan et al., 2015), а именно: предупреждения доступа злоумышленника в зону защиты; предупреждение нескрытного наличия объекта защиты в зоне защиты, предупреждение совершения злоумышленного действия в зоне защиты, локализация злоумышленного действия и ликвидация последствий злоумышленного действия.

* Corresponding author
E-mail addresses: simsim58@mail.ru (S.Zh. Simavoryan), oppm@mail.ru (A.R. Simonyan), elenaulitina@mail.ru (E.I. Ulitina), kopyrin_a@mail.ru (A.S. Kopyrin), margarita_kardashyan@mail.ru (M.A. Kardashyan), vkopeva@list.ru (V.V. Kopyeva)

2. Результаты

Рис. 1. Структура общего алгоритма динамического управления деятельностью службы физической защиты информации

В статье С.Ж. Симаворяна (Simavoryan et al., 2018) сформулирован перечень задач по построению интеллектуальных систем физической защиты информации в АСОД на базе системно-концептуального подхода. Сформулированы перечни функций и задач защиты для охранной службы АСОД с целью осуществления оперативно-диспетчерской деятельности. Разработан алгоритм задачи выбора задач защиты, практическое применение которой значительно повысит эффективность деятельности охранной службы АСОД.

Так, например, в статье В.Н. Костина, А.С. Боровского (Костин, Боровский, 2016) рассмотрен информационный подход к формированию организационных структур элементов систем физической защиты информации. Суть этого подхода заключается в том, что на рубежах проникновения нарушителей средства, осуществляющие контроль доступа в зоны защиты по количественному составу, объединяются в группы таким образом, чтобы получить оптимальное объединение этих средств по принципу равномерной информационной нагрузки на элементы управления физической защиты. Такой подход обеспечивает приспособленность системы управления в условиях неопределенности злоумышленных действий.

Перед службой физической защиты информации всегда стоит задача корректировки и совершенствования планов и механизмов защиты информации. Необходимость корректировки и совершенствования планов и механизмов связана с возникновением особо опасных и опасных ситуаций. При наступлении этих ситуаций необходимо немедленное вмешательство службы защиты. Характерным для таких ситуаций будет острый дефицит времени и отсутствие возможностей всестороннего и глубокого анализа ситуации. Поэтому необходимо заблаговременно и жестко регламентировать все действия, осуществляемые службой защиты и конкретных специалистов, непосредственно участвующих в локализации и ликвидации несанкционированного вторжения. При этом, как правило, в особо опасных

ситуациях будет иметь место психологическое напряжение. Поэтому для обеспечения достаточно высокой надежности принятия решений, целесообразно на рабочих местах службы защиты иметь схему действий в виде стенда, приведённого на Рисунке 2. При анализе опасных ситуаций дефицит времени в общем случае будет менее острым, поэтому можно будет провести более глубокий анализ ситуации, хотя времени на её детальный анализ может и не быть. С целью регламентации действий и снижения отрицательных воздействий психологической напряжённости может быть использована блок схема, возможная структура и содержание которой представлены на Рисунке 3.

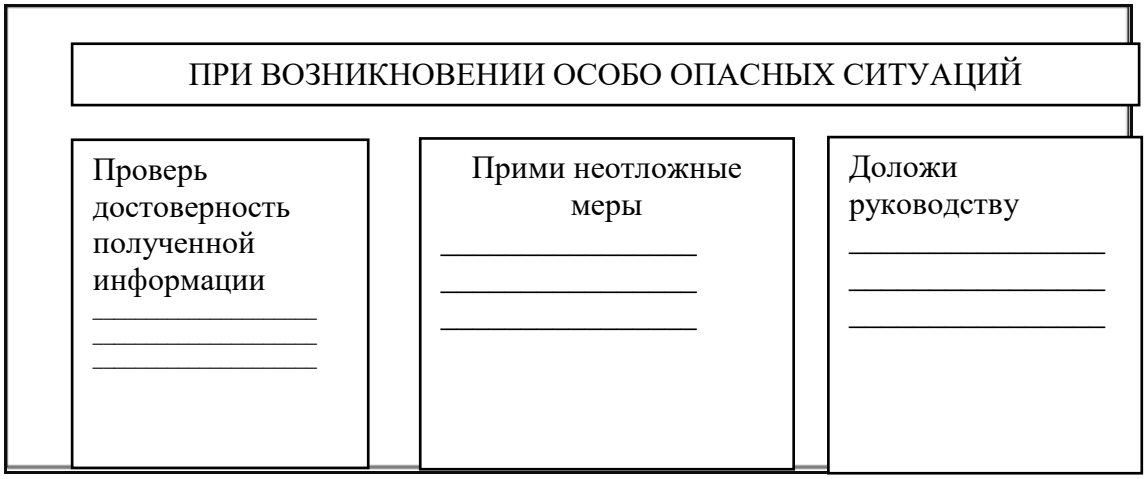

Рис. 2. Форма стенда для обеспечения принятия решений в особо опасных ситуациях

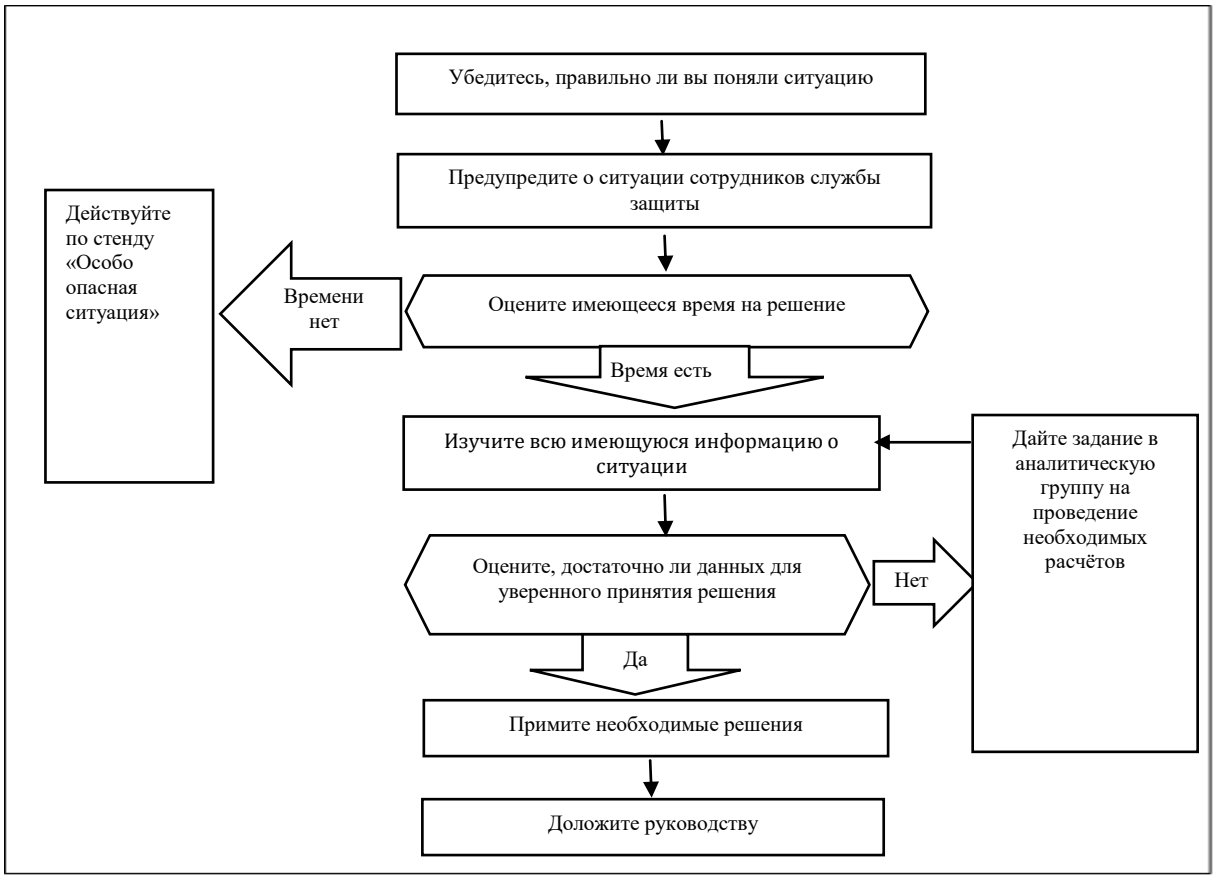

Рис. 3. Блок-схема анализа опасных ситуаций

В работах Г.А. Попова, С.В. Белова, А.В. Мельникова (Белов, Попов, 2005; Белов, Мельников, 2014) решается задача моделирования процессов и систем физической защищенности объекта защиты. Злоумышленное проникновение на объект защиты моделируется с помощью графа, отображающего возможные маршруты злоумышленного проникновения к защищаемым на объекте структурным компонентам. Оцениваются следующие характеристики: минимальное и среднее время, в течение которого происходит проникновение на объект защиты. На основе графического представления решаются задачи оценки среднего ожидаемого времени до ближайшего момента возможного проникновения злоумышленника на объект защиты, и выявления наиболее незащищенных маршрутов проникновения злоумышленника к защищаемым структурным компонентам АСОД. Предлагаемые формализованные методы анализа характеристик, описывающих уровень обеспечения безопасности объекта, позволяют более объективно и более точно оценить состояние безопасности на объекте защиты. Для повышения квалификации сотрудников службы физической защиты информации рекомендуется использовать разработанные алгоритмы по выявлению наиболее опасных маршрутов проникновения злоумышленников.

В работе Ш.Г. Магомедова и др. (Магомедов и др., 2017) рассмотрена и решена задача, связанная с охраной объектов в двух направлениях: 1) охрана объектов с помощью охранных групп, и 2) охрана объектов с использованием современных технических средств охраны. Произведены оценки издержек и потерь, связанных со степенью защищенности внешних параметров объекта защиты от возможных несанкционированных действий. Получены соотношения для средних издержек и потерь, связанных с каждой из этих служб, а также вероятности преодоления нарушителем внешнего периметра объекта, несмотря на попытки противодействия служб физической защиты. Для системы защиты введены новые характеристики – показатели надежности и квалификации сотрудника службы охраны, которые учитываются в процессе оценок. При анализе вероятностных характеристик, использовались эвристические выводы, связанные с охранными действиями.

Уместно будет привести вероятностные оценки злоумышленных действий в АСОД, приведённые в статье С.Ж. Симаворяна (Симаворян, 2009). Вероятность при некоторой {i*} совокупности злоумышленных действий, некоторой {j*} совокупности типовых объектов защиты (ТОЗ) и некоторой {γ*} совокупности нарушителей определяется как

$$P_{\{i^*\}\{j^*\}\{\gamma^*\}} = 1 - \prod_{\{i^*\}} P^{б}_{ij\gamma} \prod_{\{j^*\}} P^{б}_{ij\gamma} \prod_{\{\gamma^*\}} P^{б}_{ij\gamma} .$$

Где: ℓ – охраняемая зона; ***i*** – злоумышленное действие, *j* – типовой объект защиты; *γ* – злоумышленник.

$P^{пд}_{j\gamma\ell}$ – вероятность предупреждения доступа злоумышленника γ-ой категории в ℓ-тую охраняемую зону *j*-го ТОЗ;

$P^{пн}_{ij\ell}$ – вероятность предупреждения намерения ***i*** -го злоумышленного действия в ℓ-ой охраняемой зоне *j*-го ТОЗ;

$P^{пс}_{ij\ell}$ – вероятность предупреждения совершения ***i*** -го злоумышленного действия в ℓ-ой зоне защиты *j*-го ТОЗ;

$P^{лок}_{ij\ell}$ – вероятность локализации ***i*** - го злоумышленного действия в ℓ-ой зоне *j*-го ТОЗ;

$P^{лик}_{ij\ell}$ – вероятность ликвидации последствий ***i*** - го злоумышленного действия в ℓ-ой зоне *j*-го ТОЗ;

$\mu_B^{\gamma\ell}$ – степень принадлежности γ-го злоумышленника нечеткому множеству В – множеству потенциально возможных злоумышленников (в ℓ-ой зоне);

$\mu_A^{ij\ell}$ – степень принадлежности -го злоумышленного действия нечеткому А – множеству потенциально возможных злоумышленных действий (в ℓ-ой зоне **j**-го ТОЗ).

Вероятность совершения -го злоумышленного действия одним нарушителем γ-ой категории в ℓ-ой зоне *j*-го ТОЗ в условиях неопределенности определяется как:

$$P^{сзд}_{ij\gamma\ell} = \left(1 - P^{пд}_{j\gamma\ell}\right) \mu_B^{\gamma\ell} \left(1 - P^{пн}_{ij\ell}\right) \mu_A^{ij\ell} \left(1 - P^{пс}_{ij\ell}\right) \left(1 - P^{лок}_{ij\ell}\right) \left(1 - P^{лик}_{ij\ell}\right)$$

Базовая вероятность -го злоумышленного действия одним нарушителем γ-ой категории по в j-ом ТОЗ определяется как

$$P^{б}_{ij\gamma} = 1 - \prod_{\ell=1}^{n} \left(1 - P^{сзд}_{ij\gamma\ell}\right), \text{ где } n - \text{количество зон защиты.}$$

В качестве исходных данных для обеспечения жизнедеятельности охранных служб необходимо наличие следующих каталогов: 1) каталога потенциально возможных злоумышленных действий; 2) каталога задач защиты; 3) каталога средств защиты. Структура и содержание этих каталогов приводится на Рисунке 4.

Структура каталога злоумышленных действий:

Идентификатор злоумышленного действия	Наименование злоумышленного действия	Объект злоумышленного действия	Зона злоумышленного действия	Время возможного проявления	Идентификаторы задач защиты, закрывающие злоумышленное действие
1	2	3	4	5	6

Структура каталога задач защиты:

Идентификатор задачи защиты	Наименование задачи	Эффективность	Стоимость	Идентификаторы злоумышленных действий, для которых решается задача защиты	Идентификаторы средств защиты, которые используются при решении задач защиты
1	2	3	4	5	6

Структура каталога средств защиты:

Идентификатор средства защиты	Наименование средства защиты	Эффективность средства защиты	Стоимость средства защиты	Надёжность средства защиты	Идентификаторы задач защиты, при решении которых используется данное средство защиты
1	2	3	4	5	6

Рис. 4. Структуры каталогов

Для регулярного обновления и пополнения перечней злоумышленных действий, рекомендуется использовать психоэвристическую программу, блок схема которой приводится на Рисунке 5. Важность методологической идентификации злоумышленных действий (рисков) для эффективного управления защитой информации подчеркивается в статье (Kopyrin et al., 2017).

На Рисунке 6 приводится блок схема психоэвристической программы по корректировке и формированию идентификаторов ссылок и взаимосвязей между злоумышленными действиями, задачами и средствами. При этом следует заметить, что основным концептуальным требованием к задачам защиты является требование их адекватности по закрытию злоумышленных действий; а основным концептуальным требованием к средствам защиты является требование их надёжности. Сформированные с помощью психоэвристических программ перечни злоумышленных действий, задач и средств должны на регулярной основе обновляться с целью эффективного обеспечения оперативно-диспетчерского управления защитой информации. Принятие решения по локализации и ликвидации злоумышленного действия осуществляется на основании выработки схем закрытия злоумышленных действий по трем каталогам. Таким образом, можно осуществлять динамическую корректировку планов с использованием задач и средств защиты, которая заключается во внесении изменений в эти планы непосредственно в ходе работы службы защиты. Необходимость такой корректировки возникает в том случае, если в процессе работы значения показателей защищенности объекта выходят за границы требуемых. В зависимости от масштабов, в которых требуется корректировка, формулируются три варианта задачи: 1) оптимизация с использованием задач и средств в отдельно взятом ТОЗ; 2) оптимизация использования задач и средств на технологическом маршруте закрытия злоумышленного действия; 3) оптимизация с использованием задач и средств для всего объекта защиты.

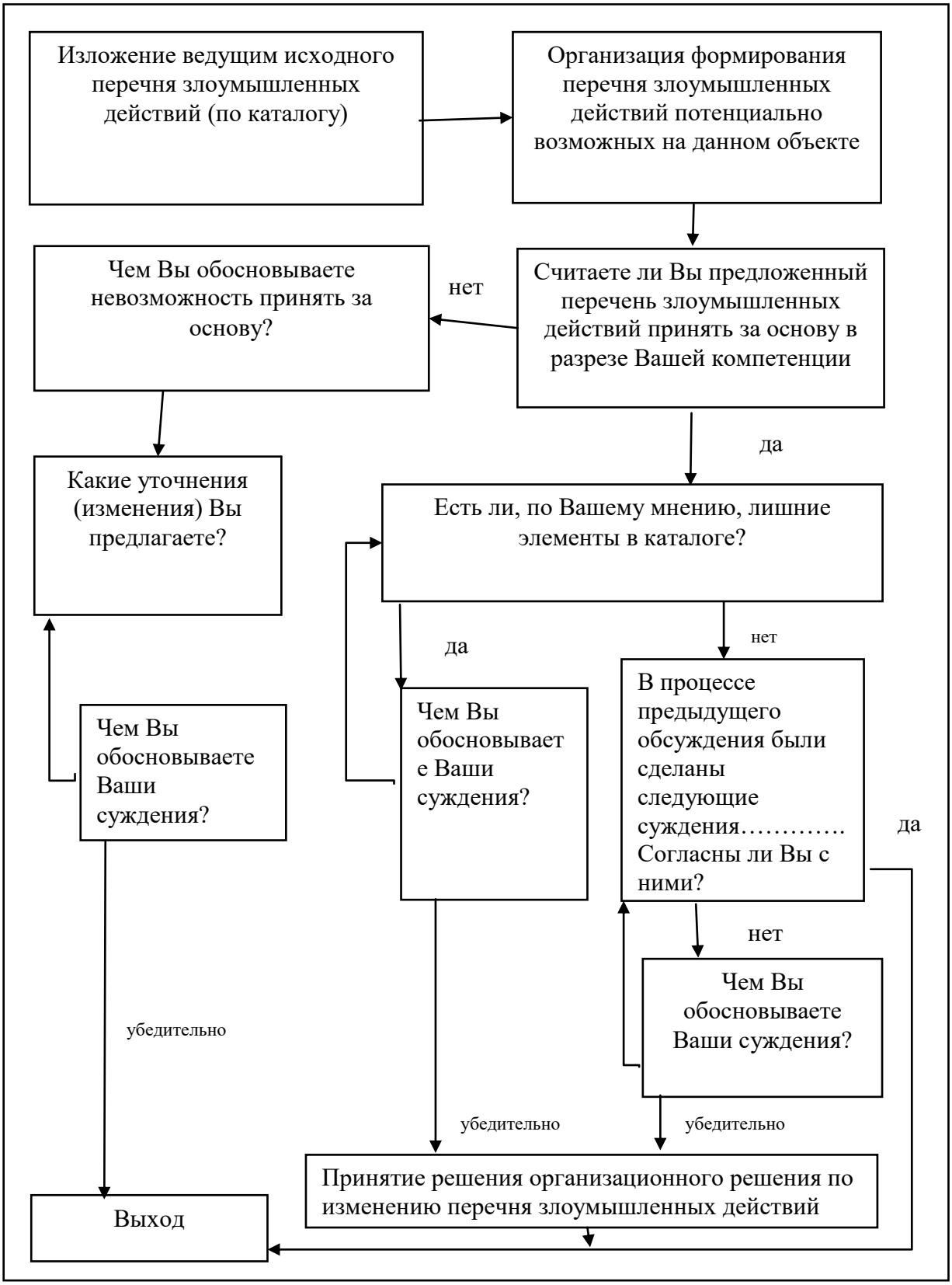

Рис. 5. Психоэвристическая программа формирования элементов каталогов

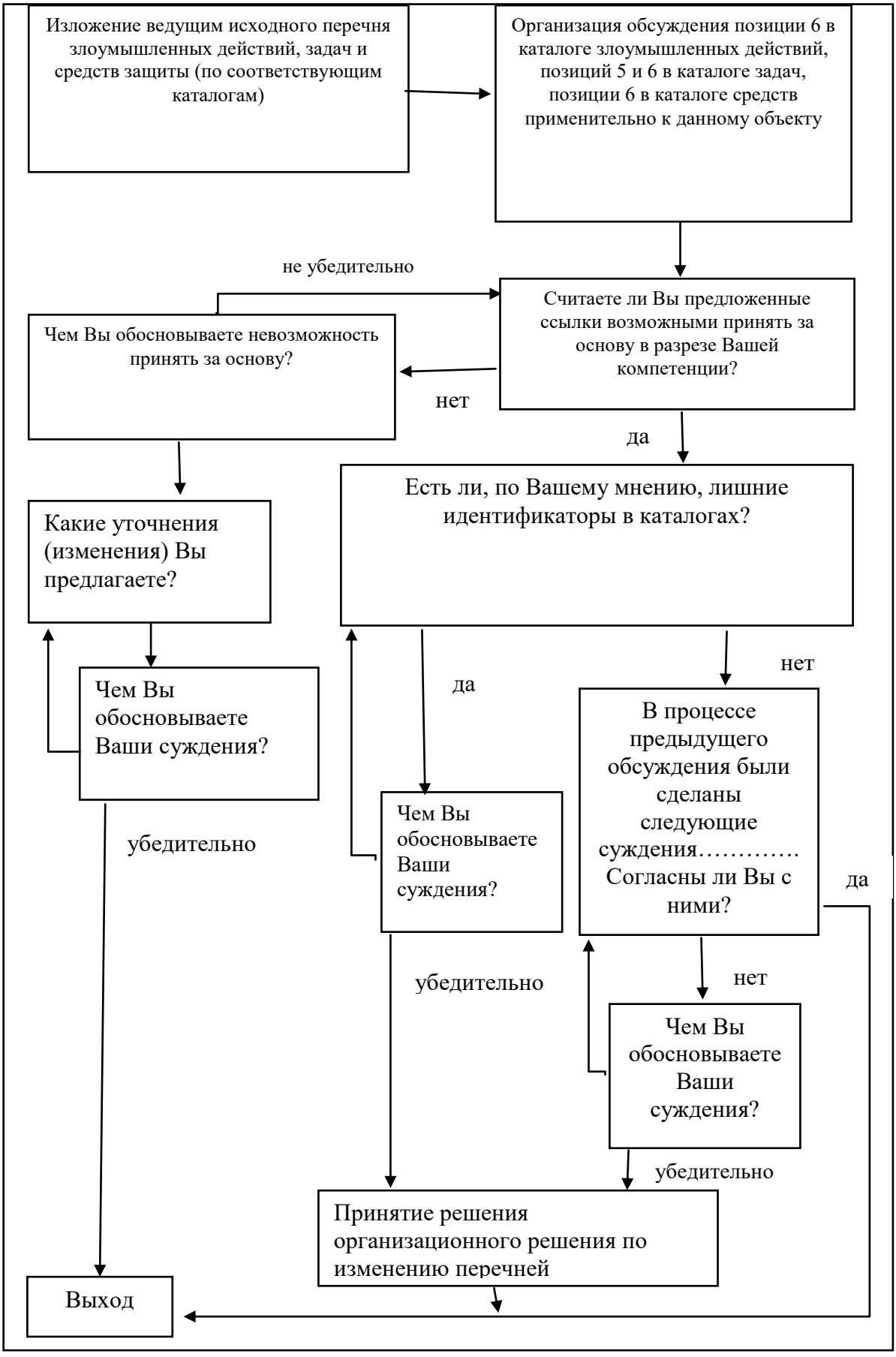

Рис. 6. Психоэвристическая программа формирования идентификаторов

3. Заключение

В работе разработан общий алгоритм динамического управления деятельностью службы физической защиты информации в АСОД. Разработана универсальная блок-схема психоэвристической программы, которая может быть использована как для формирования каталога злоумышленных действий, так и для каталогов задач и средств защиты. Разработанный алгоритм позволяет динамически перейти к внедрению интеллектуальных методов управления деятельностью службы физической защиты информации в АСОД.

4. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-01-00527.

Литература

Аверченков, Рытов, 2016 – *Аверченков В.И., Рытов М.Ю.* Служба защиты информации: организация и управление. М., 2016. (3-е издание, стереотипное).

Белов, Мельников, 2014 – *Белов С.В., Мельников А.В.* Процедура оценки показателей злоумышленного проникновения в составе автоматизированной системы контроля физической безопасности объекта защиты // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*, 2014. № 2. С. 28-37.

Белов, Попов, 2005 – *Белов С.В., Попов Г.А.* (2005). Оценка степени физической защищенности объекта защиты // *Известия высших учебных заведений. Северокавказский регион. Серия: Технические науки*, 2005. № 2. С.3-6.

Герасименко, Малюк, 1997 – *Герасименко В.А., Малюк А.А.* Основы защиты информации. М.: МИФИ, 1997. 537 с.

Герасименко, Милославская, 1997 – *Герасименко В.А., Милославская Н.Г.* Создание системы дистанционной поддержки информационной безопасности критических технологий. 1997. Отчет о НИР № 97-07-90049 (Российский фонд фундаментальных исследований).

Костин, Боровский, 2016 – *Костин В.Н., Боровский А.С.* Оптимизация организационной структуры системы физической защиты (СФЗ) на основе информационного подхода // *Информационные технологии и системы*. 2016. С. 181-185.

Магомедов и др., 2017 – *Магомедов Ш.Г., Шуршев В.Ф., Попов Г.А., Дорохов А.Ф., Руденко М.Ф.* Построение моделей описания рисков охранных действий по защите внешних периметров организации // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*, 2017. № 3. С. 31-39.

Пономаренко, 2010 – *Пономаренко С.А.* Организация и управление службой защиты информации. Уч. пособие. Образовательное учреждение высшего проф. образования "Белгородский ун-т потребительской кооперации". Белгород, 2010.

Симаворян, 2009 – *Симаворян С.Ж.* Аналитическая модель определения показателя уязвимости информации в автоматизированных системах обработки информации (АСОД) // *Обозрение прикладной и промышленной математики,* 2009. Т. 16. № 6. С. 1114.

Kopyrin et al., 2017 – *Kopyrin A.S., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* The methodology of risk analysis in assessing information security threats // *Modeling of Artificial Intelligence*, 2017. № 4-2 (2). pp. 78-85.

Simavoryan et al., 2015 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* Projecting Intelligent Systems to Protect Information in Automated Data Processing Systems (Functional Approach) // *Modeling of Artificial Intelligence,* 2015, Vol (7), Is. 3, pp. 212-220.

Simavoryan et al., 2018 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Pilosyan E.A., Simonyan R.A.* Construction of Intelligent Systems of Physical Protection of Information // *Modeling of Artificial Intelligence*, 2018, 5(1): 38-53.

References

Averchenkov, Rytov, 2016 – *Averchenkov V.I., Rytov M.Yu.* (2016). Sluzhba zashchity informatsii: organizatsiya i upravlenie [Information security service: organization and management]. M. (3-e izdanie, stereotipnoe). [in Russian]

Belov, Mel'nikov, 2014 – *Belov S.V., Mel'nikov A.V.* (2014). Protsedura otsenki pokazatelei zloumyshlennogo proniknoveniya v sostave avtomatizirovannoi sistemy kontrolya fizicheskoi bezopasnosti ob"ekta zashchity [The procedure for assessing the indicators of malicious penetration as part of an automated system for monitoring the physical security of the object of protection]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*, № 2. pp. 28-37. [in Russian]

Belov, Popov, 2005 – *Belov S.V., Popov G.A.* (2005). Otsenka stepeni fizicheskoi zashchishchennosti ob"ekta zashchity [Assessment of the degree of physical security of the object of protection]. *Izvestiya vysshikh uchebnykh zavedenii. Severokavkazskii region. Seriya: Tekhnicheskie nauki,* № 2, pp. 3-6. [in Russian]

Gerasimenko, Malyuk, 1997 – *Gerasimenko V.A., Malyuk A.A.* (1997). Osnovy zashchity informatsii [Basics of information security]. M.: MIFI. 537 p. [in Russian]

Gerasimenko, Miloslavskaya, 1997 – *Gerasimenko V.A., Miloslavskaya N.G.* (1997). Sozdanie sistemy distantsionnoi podderzhki informatsionnoi bezopasnosti kriticheskikh tekhnologii [The creation of a system of remote monitoring of the information security of critical fractures]. Otchet o NIR № 97-07-90049 (Rossiiskii fond fundamental'nykh issledovanii). [in Russian]

Kopyrin et al., 2017 – *Kopyrin A.S., Simavoryan S.Zh., Simonyan A.R., Ulitina E.I.* (2017). The methodology of risk analysis in assessing information security threats. *Modeling of Artificial Intelligence*, № 4-2 (2). pp. 78-85.

Kostin, Borovskii, 2016 – *Kostin V.N., Borovskii A.S.* (2016). Optimizatsiya organizatsionnoi struktury sistemy fizicheskoi zashchity (SFZ) na osnove informatsionnogo podkhoda [Optimization of the organizational structure of the physical protection system (PPS) based on the information approach. Information Technologies and Systems]. *Informatsionnye tekhnologii i sistemy*. pp. 181-185. [in Russian]

Magomedov i dr., 2017 – *Magomedov Sh.G., Shurshev V.F., Popov G.A., Dorokhov A.F., Rudenko M.F.* (2017). Postroenie modelei opisaniya riskov okhrannykh deistvii po zashchite vneshnikh perimetrov organizatsii [Building models describing the risks of security actions to protect the external perimeters of the organization]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika,* № 3. pp. 31-39. [in Russian]

Ponomarenko, 2010 – *Ponomarenko S.A.* (2010). Organizatsiya i upravlenie sluzhboi zashchity informatsii [Organization and management of information security service]. Uch. posobie. Obrazovatel'noe uchrezhdenie vysshego prof. obrazovaniya "Belgorodskii un-t potrebitel'skoi kooperatsii". Belgorod. [in Russian]

Simavoryan et al., 2015 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* (2015). Projecting Intelligent Systems to Protect Information in Automated Data Processing Systems (Functional Approach). *Modeling of Artificial Intelligence,* Vol (7), Is. 3, pp. 212-220.

Simavoryan et al., 2018 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Pilosyan E.A., Simonyan R.A.* (2018). Construction of Intelligent Systems of Physical Protection of Information. *Modeling of Artificial Intelligence*, 5(1): 38-53.

Simavoryan, 2009 – *Simavoryan S.Zh.* (2009). Analiticheskaya model' opredeleniya pokazatelya uyazvimosti informatsii v avtomatizirovannykh sistemakh obrabotki informatsii (ASOD) [Analytical model for determining the information vulnerability index in automated information processing systems (ASOD)]. *Obozrenie prikladnoi i promyshlennoi matematiki,* T. 16. № 6. P. 1114. [in Russian]

Структура общего алгоритма динамического управления деятельностью службы физической защиты информации в АСОД

Симон Жоржевич Симаворян [a, *], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a], Андрей Сергеевич Копырин [a], Маргарита Аркадьевна Кардашян [a], Валентина Викторовна Копьева [a]

[a] Сочинский государственный университет, Российская Федерация,

Аннотация. Работа посвящена разработке общего алгоритма динамического управления деятельностью службы физической защиты информации в АСОД. Для эффективного осуществления деятельностью службы защиты предложена универсальная блок-схема психоэвристической программы по формированию каталогов злоумышленных действий, задач защиты и средств защиты. Регулярное использование психоэвристической программы в деятельности службы защиты обеспечивает следующее: 1) обучение службы защиты; 2) актуализацию действующих каталогов: злоумышленных действий, задач и средств защиты.

Ключевые слова: физическая защита информации, психоэвристическая программа, вероятность злоумышленных действий, средства защиты, служба защиты информации.

[*] Корреспондирующий автор
Адреса электронной почты: simsim58@mail.ru (С.Ж. Симаворян), oppm@mail.ru (А.Р. Симонян), elenaulitina@mail.ru (Е.И. Улитина), kopyrin_a@mail.ru (А.С. Копырин), margarita_kardashyan@mail.ru (М.А. Кардашян), vkopeva@list.ru (В.В. Копьева)