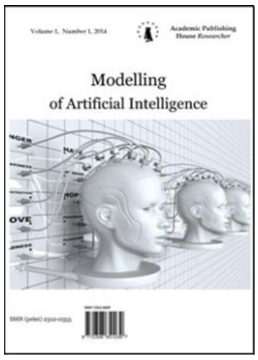

Published in the Slovak Republic
Modeling of Artificial Intelligence
Has been issued since 2014.
E-ISSN: 2413-7200
2018, 5(1): 38-53

DOI: 10.13187/mai.2018.1.38
www.ejournal11.com

Construction of Intelligent Systems of Physical Protection of Information

Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a], Irina L. Makarova [a], Elina A. Pilosyan [a], Rafael A. Simonyan [a]

[a] Sochi State University, Russian Federation

Abstract

One of the most important tasks of intelligent information security systems (IISS) automated data processing systems (ADPS) is the task of building intelligent systems of physical protection of information (ISPP). At present, the task of building ISPP is urgent, requiring systematic and regular decisions on an ongoing basis. At present, there are a lot of mathematical models and practical approaches to solving the problem of the effective functioning of physical protection systems. One interesting approach to this problem are: 1) an integrated approach to develop a mathematical model of the operation of physical protection systems (Ignat'ev, 2012; Godyreva i dr., 2007); 2) multiagent system (MAS) and technology (MAS-technology) (Shreider, Borovskii, 2017; Smirnov i dr., 2018; Gorodetskii i dr., 2017; Tarasov, 2010; Zubareva i dr., 2016). However, analysis of the regulatory basis of physical security, conducted by (Filippov, 2017) shows that the methodology for categorizing, analyzing threats and vulnerabilities differ vagueness of the conceptual apparatus and the lack of a unified terminological approach. In addition, the stresses that the analysis of threats often do not consider the connection between vulnerability and offending patterns. Not compiled a database of current security threats and vulnerabilities. However, it should be noted that the system of physical protection of critical infrastructure is largely dependent on the quality of the selection means of physical protection, and in (Yannikov i dr., 2017) proposed, developed with the help of MS SQL Server Express database "means the physical protection of critical infrastructure." Practice shows that the design methodology ISFZ built by different developers on different methodological foundations, which is dictated by different departments ADPS. Accordingly, in this paper formulated the task of building intelligent systems of physical protection of information on the basis of system-conceptual approach (Simavoryan i dr., 2013; Gerasimenko, Malyuk, 1997) worked out some aspects of its system solutions.

Keywords: physical protection of information, intellectual protection system information, system approach, system of physical protection.

1. Введение

Среди угроз, направленных на дестабилизацию работы АСОД, можно выделить угрозы связанные с возможностью проникновения злоумышленников на объекты АСОД как с целью несанкционированного доступа к возможным каналам несанкционированного

* Corresponding author
E-mail addresses: simsim58@mail.ru (S.Zh. Simavoryan), oppm@mail.ru (A.R. Simonyan), elenaulitina@mail.ru (E.I. Ulitina), ratton@mail.ru (I.L. Makarova), azalto@mail.ru (E.A. Pilosyan), raf55@list.ru (R.A. Simonyan)

получения информации (ВКНПИ), т.е. к защищаемой информации, так и с целью диверсии на объектах АСОД. Системы, которые противодействуют этому, называются системами физической защиты. Системы физической защиты представляют собой комплекс организационных мероприятий и совокупность средств, препятствующих проникновению злоумышленников на объект защиты, к его структурным компонентам, и к циркулирующей, обрабатываемой и хранимой информации.

В соответствии с работами (Шрейдер, Боровский, 2017; Simavoryan et al., 2015a) систему физической защиты можно представить в виде многоуровневой и многоблочной системы. Такой подход позволяет систему физической защиты представить в виде многоагентной системы где, все агенты взаимодействуют между собой по определенным правилам, описанным в виде должностных инструкций (Шрейдер, Боровский, 2017). Для таких систем необходимо выполнение следующих условий:

- все элементы системы и связи между ними должны быть определены до этапа проектирования;
- все элементы системы и связи между ними не изменяются во время выполнения;

Однако, следует различать:

а) системы, в которых не допускается возможность конфликтов между элементами системы;

б) системы с возможностью конфликтов между элементами системы – это системы, в которых возможен инсайд, т.е. наличие возможного злоумышленника в службе защиты информации (сговор злоумышленника и сотрудника службы защиты информации или внедрение злоумышленника в службу защиты информации).

В данной статье приводится составленный перечень задач построения интеллектуальных систем физической защиты информации на базе системно-концептуального подхода, и приводится решение задачи выбора задач защиты объекта от злоумышленных действий (вторжений) без возможности конфликтов между элементами системы.

2. Обсуждение

Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников (Игнатьев, 2012). К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио-радиотехнические и другие устройства, предназначенные для предотвращения таких несанкционированных действий как: 1) доступ (вход, выход) в зоны и помещения; 2) хищение, подмена-замена, пронос, фотографирование, копирование средств и материалов, и других компонент охраняемого объекта; 3) доступ к ВКНПИ с целью копирования и хищения секретной информации.

Физические средства применяются для решения следующих задач:

1) охрана территории АСОД и наблюдение за ней;
2) охрана зданий, внутренних помещений и контроль за ними;
3) охрана ресурсов АСОД (оборудования, информации и т.п.);
4) осуществление контролируемого доступа в здания и помещения;
5) осуществление санкционированного доступа к ВКНПИ.

В соответствии с функциями защиты информации рассмотренными в (Simavoryan et al., 2015b; Попов, Попова, 2018) все физические средства защиты объектов можно разделить на следующие категории:

- средства предупреждения доступа злоумышленника в зону защиты информации;
- средства обнаружения ВКНПИ в зоне защиты информации;
- средства обнаружения злоумышленных действий в зонах защиты;
- средства сигнализации о злоумышленных действиях;
- средства локализации последствий злоумышленных действий;
- средства ликвидации последствий злоумышленных действий.

В классическом понимании структура интеллектуальной системы включает три основных блока - базу знаний, механизм вывода решений и интеллектуальный интерфейс (Аверкин и др., 1992).

Системное решение построения ИСФЗ достигается решением последовательности следующих задач:

1. Анализ рубежей и зон защиты информации в АСОД;
2. Анализ требований и условий по защите рубежей и зон защиты;
3. Анализ возможных путей и схем преодоления злоумышленником рубежей защиты информации;
4. Анализ несанкционированных передвижений в зонах защиты;
5. Анализ охранных функций защиты информации;
6. Анализ наличия ВКНПИ в зонах защиты информации и возможных вариантов доступа к ним злоумышленников (связь уязвимости и моделей нарушителей);
7. Анализ охранных задач защиты информации;
8. Анализ средств физической защиты.
9. Анализ охранных и охранно-пожарных систем;
10. Анализ системы охранного телевидения;
11. Анализ системы охранного освещения;
12. Обоснование структуры и технологических схем функционирования охранной службы защиты информации;
13. Расчёт технико-экономических показателей системы физической защиты информации;
14. Решение организационно-правовых вопросов системы физической защиты информации.

Общая модель защиты информации состоит из следующих зон защиты: физической - внешняя, территории, помещений, ресурсов АСОД и программной - база данных (Герасименко, Малюк, 1997; Simavoryan et al., 2016a). Такой подход позволяет просчитать уязвимость информации в каждой зоне защиты информации, по каждому ВКНПИ, по каждому типовому структурному компоненту и типу злоумышленников (Симаворян, 2009a). Зоны защиты разделены между собой периметром защиты. Периметр - внешняя граница защищаемой территории зон защиты. Защита периметра – комплексная задача (Городецкий и др., 2017; Магомедов, 2018; Шанаев, 2010; Шанаев, 2009; Петров, 2008; Рытов и др., 2015; Петров, 2010; Симаворян, 2010). Эффективная защита периметра осуществляется с помощью решения следующих задач:

- контроль периметра на всём протяжении периметра, т.е. всех участках, где разрешён проход и где не разрешён проход;
- контроль и регистрация разрешённых проходов;
- обнаружение нарушения на участках, где нет разрешённого прохода;
- сигнализация нарушений;
- локализация обнаруженных нарушений;
- ликвидация последствий.

Поскольку защита информации имеет системный и многоуровневый характер, то и защита на физическом уровне должна быть системной и многоуровневой. Современные службы защиты информации, а также сотрудники АСОД всех должностей обязаны быть не просто технически образованными в области защиты информации, но и прекрасно разбираться в первую очередь в физической защите информации, которая является самой доступной и обязательной для всех. В первую очередь, в правовых вопросах необходимости применения охранных, охранно-пожарных, телевизионных и других средств защиты информации. Только благодаря регулярному повышению обучению с целью повышения квалификации сотрудников службы защиты (Симаворян, 2010; Simavoryan, 2011) можно будет добиться их адекватной должностной компетенции, которая будет необходима при аттестации или при приёме на работу на всех предприятиях АСОД в соответствии с должностным уровнем сотрудника.

Анализ разработанных моделей потенциального злоумышленника показывает, что большинство задач моделирования ИСФЗИ носит ординарный и полуординарный характер, т.е. структурированный и слабоструктурированный с одним или несколькими критериями оптимизации (Боровский, Тарасов, 2011a; Боровский, Тарасов, 2011b; Боровский, Тарасов, 2011c; Боровский, 2016; Шрейдер, Боровский, 2017; Смирнов и др., 2018; Городецкий и др., 2017; Тарасов, 2010; Магомедов, 2018; Шанаев, 2010; Шанаев, 200; Петров, 2008; Рытов и

др., 2015; Петров, 2010; Магомедов, 2018; Шанаев, 2010; Шанаев, 2009). На разработку методов и средств их решения существенное влияние оказывают следующие неопределённости (Симаворян, 2009b): неизвестность, неполнота, недостаточность, неадекватность и недостоверность. Например, неизвестность планов противника, неадекватность имеющихся моделей защиты от проникновения злоумышленника в зоны защиты, недостаточность требований по защите информации и т.д. Недостоверность делится на физическую и лингвистическую неопределённости. Источником физической неопределённости является внешняя среда, а именно злоумышленник, наличие неточностей при определении величин с помощью вычислений (измерений) физическими приборами, и наличие случайных событий, связанных со злоумышленными действиями. Источником лингвистической неопределённости является язык, используемый лицами, принимающими решения для системы управления деятельностью службы защиты информации. Лингвистическая неопределённость порождается с одной стороны, многозначностью значений слов (понятий и отношений) языка, т.е. полисемией, а с другой стороны неоднозначность смысла фраз. Если отображаемые одним и тем же словом объекты системы защиты различны, то имеет место ситуация омонимии, если сходны, то ситуация нечёткости (расплывчатости, размытости, неясности). Неоднозначность смысла фраз может быть синтаксической или семантической.

Задача анализа возможных путей и схем преодоления злоумышленником рубежей защиты информации и проникновения в зоны защиты связана с задачей анализа технологических схем функционирования информации в АСОД, которая в статье (Simavoryan et al., 2017) решена с помощью применения метода нечеткого динамического программирования. И как следствие, с задачами интеллектуального противоборства злоумышленников и службы защиты информации, которые в статье (Simavoryan et al., 2016a) решена с помощью методов итераций, а в статье (Simavoryan et al., 2016b) решена с помощью методов автоматической классификации. В работе (Тумуров и др., 2016) за основу взято понятие модели нарушителя, определенное в стандарте Банка России СТО БР ИББС-1.0–2014 (Стандарт банка России...), согласно которому модель злоумышленника определяется как описание и классификация нарушителей информационной безопасности (ИБ), включающая такие составляющие как: а) опыт, б) знания, в) доступные ресурсы, необходимые для реализации несанкционированного действия, г) мотивация и д) способы реализации угроз ИБ со стороны указанных нарушителей. Классификация злоумышленников производится следующим образом:

- внутренний – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам;
- внешний – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
- комбинированный – внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно.

В работе (Стефаров, Жуков, 2012) в соответствии с результатами анализа данных о критериях классификации нарушителей, при построении модели нарушителя предложено использовать следующие классификационные признаки: место воздействия нарушителей, мотивы действия нарушителя, каналы атак, средства атак, возможность сговора различных категорий нарушителей, наличие доступа к штатным средствам, уровень знаний нарушителей об объектах атак, уровень квалификации нарушителей, уровни воздействия нарушителей и стадии жизненного цикла автоматизированной системы. Приведена типовая модель нарушителя, учитывающая требования государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России, что позволяет применять данную модель при защите государственных информационных ресурсов, для защиты которых требования государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России являются обязательными для исполнения. Кроме того, предложенная классификация нарушителей позволяет однозначно классифицировать нарушителей в соответствии с уровнями их воздействия, чего не было представлено ранее в существующих моделях.

В рамках системно-концептуального подхода системообразующим компонентом концепции, предназначенным для обеспечения гарантированной защиты, является множество функций. Причем под функцией защиты понимается совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в АСОД различными средствами и методами с целью создания, поддержания и обеспечения условий, объективно необходимых для надёжной защиты информации (Герасименко, Малюк, 1997). Суть системного подхода к формированию функций защиты информации заключается в следующем (Simavoryan et al., 2015a; Янников и др., 2017; Попов, Попова, 2018): 1) число формируемых функций должно быть, небольшим и концептуально полным; 2) каждая функция должна описывать свои должностные особенности службы защиты информации и отличаться от других функций; 3) совокупность всех функций управления деятельностью охранной службы защиты информации не должна противоречить единству всех функций защиты информации; 4) по своей сущности в процессе их выполнения все функции должны быть однозначно трактуемыми.

Охранная деятельность службы защиты информации является частью оперативно-диспетчерского управления деятельностью АСОД. Применительно к деятельности службы защиты информации охранные функции можно сформулировать в контексте осуществления ОДУ деятельности АСОД следующим образом (Simavoryan et al., 2015b):

функция №1 – функция формирования исходных данных (сбор данных о состоянии периметров безопасности и сбор данных о состоянии передвижений и происходящих процессах в зонах защиты информации);

функция №2 – функция анализа и контроля пересечений рубежей защиты;

функция №3 – функция анализа и контроля передвижений в зонах защиты;

функция №4 – функция выработки управленческих решений;

функция №5 – функция реализация принятых решений;

функция №6 – функция сигнализации о несанкционированных действиях;

функция №7 – функция локализации несанкционированных действий;

функция №8 – функция ликвидации последствий несанкционированных действий;

функция №9 – функция контроля результатов реализации принятых решений.

Осуществление охранных функций службы защиты в АСОД достигается решением охранных задач защиты. По аналогии с определением задач защиты информации будем понимать, что под охранной задачей защиты понимаются организационные возможности средств, методов и мероприятий, реализуемых в АСОД с целью полного или частичного выполнения одной или нескольких охранных функций защиты в одной или нескольких зонах защиты (Герасименко, Малюк, 1997).

Задачи, решаемые системой охраны периметра, относятся в основном к задачам обнаружения (Петров, 2010; Шанаев, 2010):

- обнаружение нарушения на участках, где нет разрешенного прохода;
- контроль и обнаружение нарушения в тех местах, где официально установлено пересечение периметра.

Система охраны периметра рассматривается как комплексная подсистема единой системы физической защиты, в состав которой

входят сотрудники охраны, физические барьеры (ограждение), сигнализационные рубежи, система контроля и управления доступом (для контроля санкционированных мест прохода/проезда) и система охранного телевидения - для дополнительного контроля проходных и для наблюдения удаленных и трудно обозреваемых участков периметра.

Сформулируем основной перечень задач для охранной службы:

Задача: 1. Непрерывный контроль и анализ ситуаций, связанных с нарушениями прохождения периметров защиты и санкционированных передвижений во всех зонах защиты информации в АСОД;

Задача 2. Непрерывный сбор, обработка и формирование интеллектуальных баз данных по ситуациям, связанным с нарушениями прохождения периметров защиты и санкционированных передвижений во всех зонах защиты информации в АСОД;

Задача 3. Контроль и анализ адекватности выполнения поставленных задач защиты в соответствии с функциями защиты;

Задача 4. Контроль и анализ надежности функционирования охранных средств защиты в соответствии с охранными задачами защиты;

Задача 5. Интеллектуальный анализ и прогнозирование развития ситуаций, связанных с нарушениями прохождения периметров защиты и санкционированных передвижений во всех зонах защиты информации в АСОД;

Задача 6. Принятие решений по оперативному и практическому контролю доступа злоумышленников в зоны защиты объекта, с возможностью, в случае необходимости, вмешательства в работу подсистемы доступа злоумышленников в зону защиты;

Задача 7. Принятие решений по оперативному и практическому контролю наличия ВКНПИ в зоне защиты информации, с возможностью, в случае необходимости, вмешательства в работу подсистемы контроля наличия ВКНПИ в зонах защиты;

Задача 8. Принятие решений по оперативному и практическому контролю наличия информации в каналах НПИ, с возможностью, в случае необходимости, вмешательства в работу подсистемы контроля наличия информации в каналах НПИ;

Задача 9. Принятие решений по оперативной и практической локализации несанкционированного прохождения периметров защиты и несанкционированных передвижений во всех зонах защиты информации в АСОД с возможностью, в случае необходимости, вмешательства в работу подсистемы контроля;

Задача 10. Принятие решений по оперативной и практической ликвидации последствий злоумышленных действий, с возможностью, в случае необходимости, вмешательства в работу подсистемы ликвидации последствий злоумышленных действий;

Задача 11. Внесение и корректировка разработанных предложений по внесению изменений в планы по ОДУ службы охраны;

Задача 12. Отработка учетно-отчетных документов, относящихся к оперативно-диспетчерской деятельности службы охраны АСОД.

Сформулируем задачу выбора задач (действий) с заданной эффективностью. Приведём её:

Найти

$X_{\xi i} = \begin{cases} 1, & \text{если } \xi\text{–ая задача используется при закрытии } i\text{–го вторжения,} \\ 0, & \text{в противном случае,} \end{cases}$

такие, что $max_{\xi}\{Э_{\xi i^*} x_{\xi i}\} \geq \bar{Э}_i$,

для всех i, при которых

$$C = \sum_{\xi=1}^{m} C_{\xi}(\text{sign} \sum_{k=1}^{n} x_{\xi k}) \rightarrow min$$

где i =1,...,n; ξ=1,...,m.

Это задача нелинейного программирования. Для решения таких задач одним из эффективных методов является метод Хука-Дживса (Методы Хука-Дживса). В зависимости от особенностей и условий задач этот метод может быть легко модифицирован и успешно применён.

Эффективность перекрытия (реагирования) -го вторжения (злоумышленного действия) решением ξ-ой задачи зависит от полноты (степени) решения самой задачи и своевременности (оперативности) реагирования. Стоимость решения задачи зависит от степени решения задачи и от стоимости используемых средств защиты. Для большинства задач, особенно тех, которые носят неформальный характер невозможно точно определить эффективность их решения $Э_{\xi i}$. Задача определения $Э_{\xi i}$ упрощается, если априорно, на основе систематизации мнений экспертов, формируются приближённые словесные описания эффективности, которые можно формализовать, используя лингвистические переменные.

Структура общей модели выбора задач реагирования на потенциально возможные злоумышленные действия приводится на Рисунке 1.

Рассмотрим содержание первого блока. Для каждой зоны защиты необходимо сформировать перечень потенциально возможных злоумышленных действий с указанием места злоумышленного действия. Такой перечень можно сформировать с помощью

психоэвристической программы, с привлечением специалистов службы безопасности и специалистов, которых можно будет назвать «условными злоумышленниками» из числа проектировщиков системы физической защиты. Психоэвристическая программа формирования потенциально возможных действий злоумышленника в данной статье не приводится. Исходными данными для такой психоэвристической программы являются данные из всевозможных каталогов злоумышленных действий, имеющихся у разработчиков и службы защиты.

Рассмотрим содержание второго блока. В этом блоке формируется матрица $\mathcal{A} = (\alpha_{\xi i})$, ξ=1,...,n; i =1,...,m. Матрица $\mathcal{A}$ отражает взаимосвязь между злоумышленным действием и перечнем задач, решаемых охранной службой защиты информации по пресечению злоумышленного действия. Матрица $\mathcal{A}$ может часто не отражать реальной ситуации по закрытию злоумышленного действия. Это может быть в силу следующих причин: 1) не всегда сотрудник службы защиты может знать о знании слабых мест в защите, следует учитывать, что злоумышленник постоянно ищет слабые места в защите; 2) в перечне (каталоге) задач, могут быть указаны не все задачи, пресекающее злоумышленное действие. Формирование матрицы $\mathcal{A}$ осуществляется для каждой зоны защиты информации, т.е. приобретает «зональный» характер. Далее все рассуждения будут вестись для одной зоны.

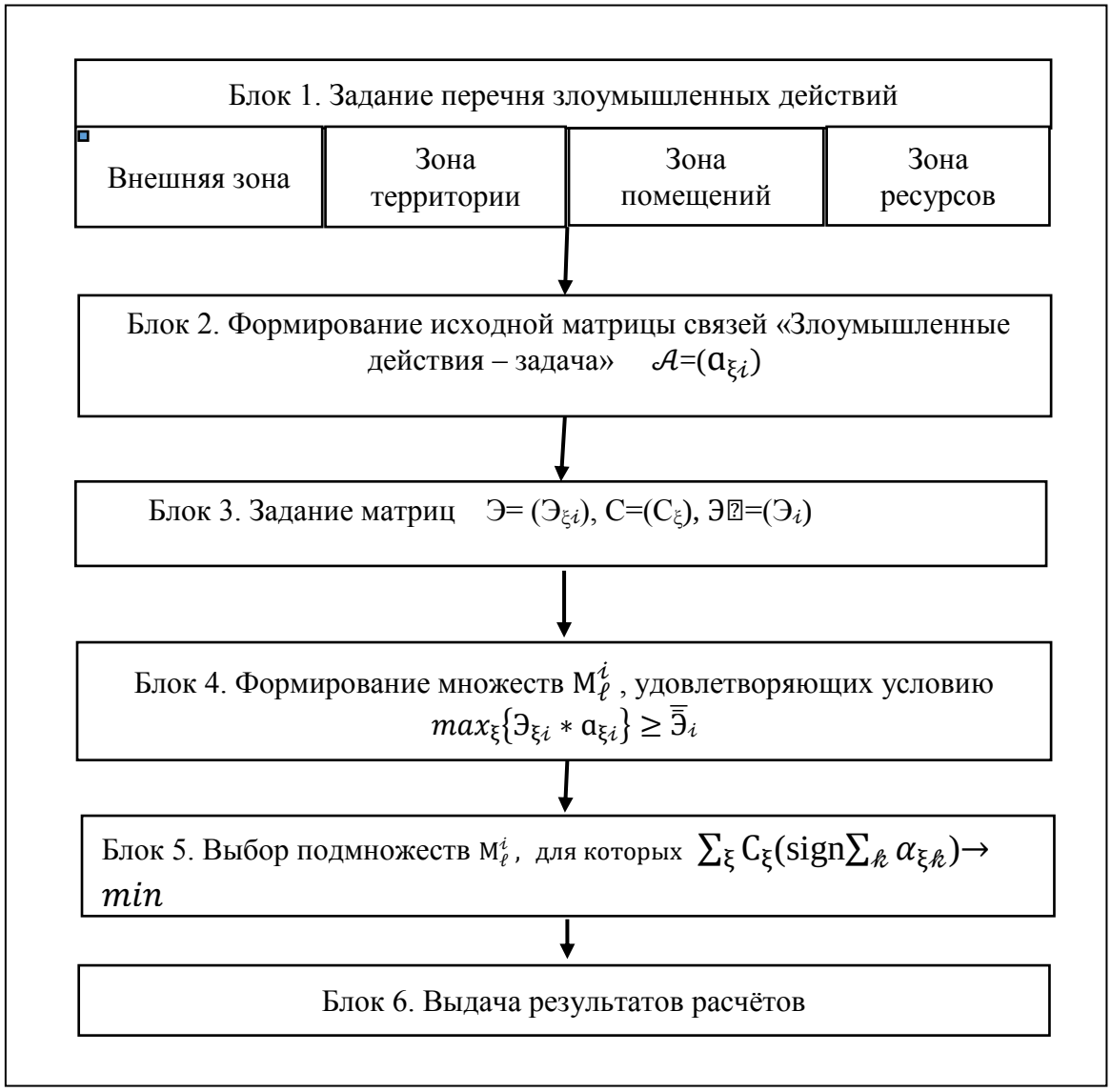

Рис. 1. Структура общей модели решения задачи выбора задач, подлежащих решению.

Рассмотрим содержание третьего блока. Формирование матриц

Э= ($Э_{\xi i}$), C=(C_ξ), Э⍰=($Э_i$), ξ=1,...,n; i =1,...,m

может быть также осуществлено с помощью психоэвристических программ, аналогичных предыдущим. Элементами этих матриц будут лингвистические переменные.

В четвёртом блоке производится формирование всевозможных множеств M_i^ℓ задач службы защиты, которые обеспечивают требуемую эффективность перекрытия i -го злоумышленного вторжения. Множество M_i^ℓ определим следующим образом:

$$M_i^\ell = \begin{cases} \emptyset, \text{если } k = 0; \\ m_i^\ell[1], m_i^\ell[2], \dots, m_i^\ell[k] \quad , \text{если } k \geq 1, \end{cases}$$

где k – последовательная индексация, max k =C_m^ℓ, $m_i^\ell[k]$ – k-ый ℓ -элементный кортеж задач защиты, обеспечивающий закрытие i –го вторжения с заданной эффективностью $\bar{Э}i$, т.е.

$$max_\xi\{Э_{\xi i} * a_{\xi i}\} \geq \bar{\bar{Э}}_i ,$$

где $m_i^\ell[k] = \{a_{\xi_\delta i}, a_{\xi_\beta i}, \dots, a_{\xi_\varphi i}\}[k]$,

$\xi_\delta, \xi_\beta, \dots, \xi_\varphi \in [0, m], a_{\xi i} = 1 \vee 0.$

Пусть $M_i = \bigcup_\ell M_i^\ell$- множество эффективных подмножеств закрытия

i -го вторжения. Необходимость формирования множества продиктована тем, что одна и та же задача закрытия вторжения может быть использована при закрытии нескольких вторжений, что очень важно учитывать при определении суммарных затрат на закрытие нескольких злоумышленных действий. Кроме того, следует учесть, что задачи имеют различную стоимость и может быть так, что стоимость решения r задач (r≥2) меньше, чем стоимость решения s задач, s<r. Опишем правила построения множества M_i .

Правило образования подмножеств.

Элементами подмножества M_i^ℓ являются ℓ -элементные кортежи, элементами кортежей являются задачи, суммарная эффективность которых не меньше требуемой.

Правило рекурсивного устранения избыточности.

Если $m_i^\ell[k]$= $\{a_{\xi_{k1}}, \dots, a_{\xi_{k\ell}}\}$ - есть k -ый кортеж подмножества M_i^ℓ, то никакие его (ℓ -1) элементов (в любом сочетании) не обеспечивают закрытия i -го вторжения с заданной эффективностью.

Введенные правила обеспечивают оптимальное построение множества M_i. Оптимальность понимается в смысле полноты M_i и отсутствия избыточности. Первое правило даёт возможность включить в подмножества M_i^ℓ все ℓ-элементные кортежи, обеспечивающие закрытие i-го вторжения с заданной эффективностью $\bar{Э}_i$. Второе правило говорит, что не существует такого $a_{\xi_\delta i}$, что

$m_i{}^{\ell+1} = m_i{}^\ell \vee a_{\xi_\delta i}$, где $m_i{}^\ell = \left\{ a^\ell_{\xi_{a_1} i}, \dots, a^\ell_{\xi_{a_\ell}} \right\}$,

$m_i{}^{\ell+1} = \left\{ a^{\ell+1}_{\xi_{a_1} i}, \dots, a^{\ell+1}_{\xi_{a_\ell}} \right\}$,

$m_i{}^\ell \in M_i^\ell$, $m_i{}^{\ell+1} \in M_i^{\ell+1}$.

Перейдём к описанию пятого блока. В предыдущем блоке были построены множества M_i^ℓ, i =1,...,n, которые представим в виде матрицы:

	M_1^1	M_1^2	…	M_1^ℓ	…
	M_2^1	M_2^2	…	M_2^ℓ	…
	M_3^1	M_3^2	…	M_3^ℓ	…
	…	…	…	…	…
-1	M_{n-1}^1	M_{n-1}^2	…	M_{n-1}^ℓ	…
	M_n^1	M_n^2	…	M_n^ℓ	…

Минимизация функции $\sum_{\xi} C_{\xi}(\text{sign}\sum_{k} \alpha_{\xi k})$ будет осуществляться по следующему алгоритму:

Шаг 1. Из каждой строки приведённой матрицы выбираются m_i^{ℓ}, из которых составляются всевозможные выборки задач защиты

R[r]= $\vee_{\ell,i,[k]} m_i^{\ell}[k]$, где r=1,2,...

Шаг 2. Вычисляется суммарная стоимость этих выборок.

Шаг 3. Из всех этих выборок выбирается выборка с наименьшей стоимостью. Если таких несколько, то выбирается выборка с минимальным количеством задач, но если и таких несколько, то по обстоятельствам выбирается выборка по желанию службы защиты.

В блоке 6 осуществляется выдача полученных результатов.

Решение задачи выбора задач даёт возможность руководству по защите, исходя из требуемой эффективности закрытия злоумышленного действия, стоимости решения задач, варьировать выборками задач. Т.е. в зависимости от смены дежурства на объекте, каждой смене может быть поставлено своё задание по обеспечению безопасности функционирования объекта, о которой предыдущая смена и знать не будет. Например, это даёт возможность говорить о механизмах (ключах) защиты объекта на уровне целой смены, т.е. каждое задание имеет свой механизм исполнения. В таких условиях злоумышленнику будет очень трудно проконтролировать работу службы защиты.

Заметим, что в наших рассуждениях (несмотря на то, что для определения эффективности решения задач использовались лингвистические переменные) подразумевается, что формирование лингвистических переменных производится при условии того, что задачи защиты решаются полностью. Если ввести коэффициент μ ($\mu \in [0,1]$) выполнения задачи, то получим реальную картину отражающую действительность, т.е. $Э_{\xi i}^{\text{новое}} = \mu * Э_i$. При $\mu = 0$ имеем, что задача практически не была решена; при $\mu = 1$ имеем, что задача решена полностью и $Э_{\xi i}^{\text{новое}} = Э_i$;при $\mu = 0{,}5$ имеем, что задача решена наполовину и $Э_{\xi i}^{\text{новое}} = 0{,}5 * Э_i$, и т.д.

Один из подходов к формализации подобных задач заключается в следующем. Допустим, что $\bar{C}$ – заданная величина стоимости, такая, что для решения задачи достаточно выполнение неравенства

$\bar{C}=\sum_{\xi} C_{\xi}\left(sign\ \sum_{k} x_{\xi k}\right) \le b$

Введем нечеткие множества целей и ограничений

$$\mu_G=(x_{\xi i})=\begin{cases} 0, \text{если } \max_{\xi}\{Э_{\xi i} * x_{\xi i}\} < \bar{Э}_i, \\ \mu(x_{\xi i}), \text{в противном случае.} \end{cases}$$

$$\mu_C=(x_{\xi i})=\begin{cases} 0, \text{если } \sum_{\xi} C_{\xi}\left(sign\ \sum_{k} x_{\xi k}\right) > b \\ \varphi(x_{\xi i}), \text{в противном случае,} \end{cases}$$

где μ и φ – некоторые функции описывающие степени выполнения соответствующих неравенств с точки зрения службы защиты. В результате чего исходная задача оказывается сформулированной в форме задачи выполнения нечётко определённой цели, к которой применим подход Беллмана-Заде (Орловский, 1981). Задачи защиты являются той основой, которая, во-первых, создаёт предпосылки перехода от обеспечения защиты к её управлению, а во-вторых, объединяет все остальные задачи, решаемые в процессе защиты в единое целое – систему задач по обеспечению защиты от вторжения. Качество работы любой сложной системы оценивается с помощью показателей эффективности. Под показателем эффективности понимается такая характеристика, которая оценивает степень приспособления системы к выполнению поставленных целей (Панов, 2013). Ясно, что основной целью решения задач охраны является надёжное закрытие потенциально возможных вторжений на охраняемый объект. Многие задачи охраны носят неформальный характер, при решении которых главным действующим лицом является человек, однако цели некоторых задач не могут быть строго формализованы и оценки защищённости объекта выражены лингвистически. Кроме того, процессы злоумышленных действий носят вероятностный характер. Таким образом, ясно, что вероятность выступая как специфическое

свойство злоумышленных действий, не является достаточным для его полной характеристики.

Таким образом, ясно, что под показателем эффективности решения задачи будем понимать степень перекрытия злоумышленного действия при решении данной задачи. Поскольку на эффективность решения задачи влияют такие факторы как степень решения задачи, вероятность безошибочной работы человека, то эффективность решения задач защиты информации может быть оценена следующим образом:

$Э_{\xi i}=\left(P_{\xi i}^{1} - P_{\xi i}^{2}\right) * R_{\xi i}{}^{*}Q_{\xi i}$,

где $Э_{\xi i}$ – эффективность решения ξ-ой задачи при закрытии i-го злоумышленного действия;

$P_{\xi i}^{1}$ – вероятность вторжения при закрытии -го злоумышленного действия решением ξ-ой задачи;

$P_{\xi i}^{2}$ - вероятность вторжения при закрытии -го злоумышленного действия без решения ξ-ой задачи;

$R_{\xi i}$ – степень решения задачи ($R_{\xi i} \in [0,1]$);

$Q_{\xi i}$ – надёжность безошибочной работы человека при закрытии -го злоумышленного действия решением ξ-ой задачи.

Надёжность безошибочной работы человека определяется как (Акимов и др., 2002):

$Q_{\xi i}(t)=e^{-\int e(t)d(t)}$,

где $e(t)$ – частота появления ошибок по вине человека в момент времени t. Поскольку $e(t)$ подчиняется экспоненциальному закону, то $e(t) = \lambda = const$, откуда $Q_{\xi i}(t)=e^{-\lambda t}$, где λ – интенсивность ошибок определяемая экспертным путём на основе накопленного опыта. Тогда формулу эффективность решения задач можно представить в виде

$Э_{\xi i}=\left(P_{\xi i}^{1} - P_{\xi i}^{2}\right) * R_{\xi i}{}^{*}e^{-\lambda t}$.

Согласно (Акимов и др., 2002) $10^{-3} \leq \lambda \leq 10^{-2}$ в зависимости от квалификации специалиста и сложности решаемых задач. Если в процессе решения задачи защиты человек практически не принимает участия, то $Q_{\xi i}(t) \equiv 1$.

3. Результаты

Сформулирован перечень задач по построению интеллектуальных систем физической защиты АСОД на базе системно-концептуального подхода. Сформулирован перечень функций защиты для охранной службы АСОД. Сформулирован перечень задач для охранной службы АСОД с целью осуществления оперативно-диспетчерской деятельности. Разработана задача выбора задач защиты, практическое применение которой значительно повысит эффективность деятельности охранной службы АСОД.

4. Заключение

Для решения поставленных в статье задач требуется: 1) составить каталог задач, выполняемых службой охраны; 2) составить каталог средств защиты для решения задач; 3) разработать механизмы их реализации; 4) постоянно на регулярной основе проводить обучение персонала охранных службы. Для решения этих задач требуется большое количество исходных данных. Эти данные, в силу особенностей для различных АСОД, составляются с помощью эвристических методов, сущность которых будет публиковаться в следующих публикациях.

5. Благодарности

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

Литература

Аверкин и др., 1992 – *Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А.* Толковый словарь по искусственному интеллекту. М.: Радио и связь, 1992. 256 с.

Акимов и др., 2002 – *Акимов В.А., Лапин В.Л., Попов В.М.* Надежность технических систем и техногенный риск. М.: ЗАО ФИД «Деловой экспресс», 2002. 368 с.

Боровский, 2016 – *Боровский А.С.* Интегрированный подход к построению систем физической защиты объектов // *Наука и образование транспорту*. 2016. № 2. С. 12-16.

Боровский, Тарасов, 2011a – *Боровский А.С., Тарасов А.Д.* Интегрированный подход к разработке общей математической модели функционирования систем физической защиты объектов // *Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии*. 2011. № 1. С. 50-59.

Боровский, Тарасов, 2011b – Боровский А.С., Тарасов А.Д. Интегрированный подход к разработке общей математической модели функционирования систем физической защиты объектов // *Информационные системы и технологии*. 2011. № 1 (63). С. 111-127.

Боровский, Тарасов, 2011c – *Боровский А.С., Тарасов А.Д.* Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов // *Труды Института системного анализа Российской академии наук*. 2011. Т. 61. № 1. С. 3-13.

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

Годырева и др., 2007 – *Годырева А.В., Николаева Т.С., Кармановский Н.С.* Основные направления обеспечения комплексной защиты информации крупных предприятий // *Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики*. 2007. № 40. С. 221-227.

Городецкий и др., 2017 – *Городецкий В.И., Бухвалов О.Л., Скобелев П.О.* Современное состояние и перспективы индустриальных применений многоагентных систем // *Управление большими системами: сборник трудов*. 2017. № 66. С. 94-157.

Зубарева и др., 2016 – *Зубарева М.Г., Цветков А.А., Хамуш А.Л., Шорох Д.К., Шуклин А.В., Юрсков С.В.* Методологии проектирования мультиагентных систем / *Технические науки в России и за рубежом Материалы VI Международной научной конференции*. 2016. С. 3-8.

Игнатьев, 2012 – *Игнатьев В.А.* Информационная безопасность современного коммерческого предприятия. Монография. Старый Оскол: ООО «ТНТ», 2012. 448 с.

Магомедов, 2018 – *Магомедов Ш.Г.* Классификация рубежей доступа и связанных с ними факторов влияния в системе контроля доступа // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2018. № 1. С. 62-70.

Магомедов, 2018 – *Магомедов Ш.Г.* Классификация рубежей доступа и связанных с ними факторов влияния в системе контроля доступа // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2018. № 1. С.62-70.

Методы Хука-Дживса – Методы Хука-Дживса. Минск: Белорусская цифровая библиотека LIBRARY.BY. Дата обновления: 04 июня 2010. URL: http://library.by/portalus/modules/different/readme.php?subaction=showfull&id=1275677296&archive=1275730016&start_from=&ucat=& (дата обращения: 29.07.2018).

Орловский, 1981 – *Орловский С.А.* Проблемы принятия решений при нечеткой исходной информации. М.: Наука. Гл. ред. физ.-мат. лит.,1981. 208с.

Панов, 2013 – *Панов М.М.* Оценка деятельности и система управления компанией на основе KPI. М.: Инфра-М, 2013. 255 с.

Петров, 2008 – *Петров Н.В.* Система охраны периметра // *Защита информации. Инсайд*. 2008. № 1 (19). С. 56-61.

Петров, 2010 – *Петров Н.В.* Обоснование выбора технических средств обнаружения для систем охранной сигнализации периметра // *Защита информации*. Инсайд. 2010. № 5 (35). С. 76-86.

Попов, Попова, 2018 – *Попов Г.А., Попова Е.А.* Системный подход к формированию состава функций управления в системах защиты информации // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2018. № 1. С. 71-80.

Рытов и др., 2015 – *Рытов М.Ю., Еременко В.Т., Гулак М.Л.* Модель процесса выбора состава технических средств систем физической защиты // *Информация и безопасность*. 2015. Т. 18. № 4. С. 502-507.

Симаворян и др., 2013 – *Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А.* Системный подход к проектированию интеллектуальных систем защиты информации // *Известия Сочинского государственного университета,* 2013, № 4-2(28), с. 128-132.

Симаворян, 2009a – *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. 1115.

Симаворян, 2009b – *Симаворян С.Ж.* Понятие неопределенности в задачах защиты информации. *Обозрение прикладной и промышленной математики*. 2009. Т. 16. № 6. С. 1115.

Симаворян, 2010 – *Симаворян С.Ж.* О необходимости преподавания дисциплины "Информационная безопасность" на гуманитарных факультетах ВУЗов // *Вестник Сочинского государственного университета туризма и курортного дела*. 2010. № 4. С. 65-73.

Смирнов и др., 2018 – *Смирнов А.В., Хабибулин Р.Ш., Тараканов Д.В.* Применение многоагентного подхода для поддержки управления безопасностью в техносфере // *Вестник Иркутского государственного технического университета*. 2018. Т. 22. № 1. С. 118–133. DOI: 10.21285/1814-3520-2018-1-118-133

Стандарт банка России... – Стандарт банка России СТО БР ИББС-1.0–2014. Обеспечение информационной безопасности организационной банковской системы Российской Федерации. Общие положения [Электронный ресурс]. URL: http://www.cbr.ru/credit/gubzi_docs/st-10-14.pdf (дата обращения: 08.06.18).

Стефаров, Жуков, 2012 – *Стефаров А.П., Жуков В.Г.* Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах // *Известия ЮФУ. Технические науки*. 2012. № 12 (137). С. 45-54.

Тарасов, 2010 – *Тарасов А.Д.* Система физической защиты на основе агентно-ориентированного подхода и нечеткой логики // *Проблемы управления и моделирования в сложных системах: материалы XII Междунар. конф. (Самара, 21–23 июня 2010 г.)*. Самара, 2010. С. 650–656.

Тумуров и др., 2016 – *Тумуров Г.В., Вознюк А.Н., Кшнянкин А.П.* Модель нарушителя подсистемы технической защиты информации объекта информатизации // *Электронные средства и системы управления*. 2016. № 1-2. С. 62-64.

Филиппов, 2017 – *Филиппов Д.Л.* Об отечественной нормативно-методической базе физической безопасности // Проблемы анализа риска. 2017. Т. 14. № 6. С. 84-87.

Шанаев, 2009 – *Шанаев Г.* Инженерные средства физической защиты периметра // *Алгоритм безопасности*. 2009. № 4. С. 6-13.

Шанаев, 2010 – *Шанаев Г.* Варианты построения рубежей охраны объекта при наличии факторов, усложняющих функционирование СЗП искусственного происхождения // *Алгоритм безопасности*. 2010. № 1. С. 56-60.

Шрейдер, Боровский, 2017 – Шрейдер М.Ю., Боровский А.С. Применение многоагентного подхода к построению систем физической защиты объектов // *Интеллект. Инновации. Инвестиции*. 2017. № 10. С. 66-71.

Янников и др., 2017 – *Янников И.М., Соболева Н.В., Куделькин В.А., Казанцев М.М., Габричидзе Т.Г.* База данных средств физической защиты потенциально опасных объектов // *Интеллектуальные системы в производстве*. 2017. Т. 15. № 1. С. 122-125.

Simavoryan et al., 2015a – *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. № 3 (7). pp. 212-220.

Simavoryan et al., 2015b – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* Research of the intellectual antagonism of malefactors and service of information security in the ADPS // *Modeling of Artificial Intelligence*. 2015. № 1 (5). pp. 33-41.

Simavoryan et al., 2016a – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* Creating the conditions for the theoretical and practical solution of the problem of

automated intelligent search for the attacker's image in ADPS // *Modeling of Artificial Intelligence*. 2016. № 3 (11). pp. 166-176.

Simavoryan et al., 2016b – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Samarin V.I., Simonyan R.A., Kardashyan M.A.* Enhancing operational efficiency of the fuzzy image of the attacker's method of iterations // *Modeling of Artificial Intelligence*. 2016. № 4 (12). pp. 187-193.

Simavoryan et al., 2017 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* The task of determining the optimal technological scheme for the operation of information security systems // *European Journal of Computer Science*. 2017. № 3 (1). pp. 17-22.

Simavoryan, 2011 – *Simavoryan S.Zh.* About application during lectures on protection of the information and information security of the method of "The round table" // *European Researcher*. 2011. № 5-1 (7). pp. 760-762.

References

Akimov i dr., 2002 – *Akimov V.A., Lapin V.L., Popov V.M.* (2002). Nadezhnost' tekhnicheskikh sistem i tekhnogennyi risk [Reliability of technical systems and technogenic risk]. M.: ZAO FID «Delovoi ekspress», 368 p. [in Russian]

Averkin i dr., 1992 – *Averkin A.N., Gaaze-Rapoport M.G., Pospelov D.A.* (1992). Tolkovyi slovar' po iskusstvennomu intellektu [Explanatory dictionary on artificial intelligence]. M.: Radio i svyaz', 256 p. [in Russian]

Borovskii, 2016 – *Borovskii A.S.* (2016). Integrirovannyi podkhod k postroeniyu sistem fizicheskoi zashchity ob"ektov [Integrated approach to the construction of physical protection systems of objects]. Nauka i obrazovanie transportu. № 2. pp. 12-16. [in Russian]

Borovskii, Tarasov, 2011a – *Borovskii A.S., Tarasov A.D.* (2011). Integrirovannyi podkhod k razrabotke obshchei matematicheskoi modeli funktsionirovaniya sistem fizicheskoi zashchity ob"ektov [An integrated approach to the development of a general mathematical model for the functioning of physical protection systems of objects]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyi analiz i informatsionnye tekhnologii*. № 1. pp. 50-59. [in Russian]

Borovskii, Tarasov, 2011b – Borovskii A.S., Tarasov A.D. (2011). Integrirovannyi podkhod k razrabotke obshchei matematicheskoi modeli funktsionirovaniya sistem fizicheskoi zashchity ob"ektov [An integrated approach to the development of a general mathematical model for the functioning of physical protection systems of objects]. Informatsionnye sistemy i tekhnologii. № 1 (63). pp. 111-127. [in Russian]

Borovskii, Tarasov, 2011c – *Borovskii A.S., Tarasov A.D.* (2011). Integrirovannyi podkhod k razrabotke obshchei modeli funktsionirovaniya sistem fizicheskoi zashchity ob"ektov [An integrated approach to the development of a general mathematical model for the functioning of physical protection systems of objects]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*. T. 61. № 1. pp. 3-13. [in Russian]

Filippov, 2017 – *Filippov D.L.* (2017). Ob otechestvennoi normativno-metodicheskoi baze fizicheskoi bezopasnosti [On the national regulatory and methodological basis of physical security]. Problemy analiza riska. T. 14. № 6. pp. 84-87. [in Russian]

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

Godyreva i dr., 2007 – *Godyreva A.V., Nikolaeva T.S., Karmanovskii N.S.* (2007). Osnovnye napravleniya obespecheniya kompleksnoi zashchity informatsii krupnykh predpriyatii [The main directions of providing comprehensive information protection for large enterprises]. Nauchno-tekhnicheskii vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta informatsionnykh tekhnologii, mekhaniki i optiki. № 40. pp. 221-227. [in Russian]

Gorodetskii i dr., 2017 – *Gorodetskii V.I., Bukhvalov O.L., Skobelev P.O.* (2017). Sovremennoe sostoyanie i perspektivy industrial'nykh primenenii mnogoagentnykh sistem [Current state and prospects of industrial applications of multi-agent systems]. Upravlenie bol'shimi sistemami: sbornik trudov. № 66. pp. 94-157. [in Russian]

Ignat'ev, 2012 – *Ignat'ev V.A.* (2012). Informatsionnaya bezopasnost' sovremennogo kommercheskogo predpriyatiya [Information security of a modern commercial enterprise]. Monografiya. Staryi Oskol: OOO «TNT», 448 p. [in Russian]

Magomedov, 2018 – *Magomedov Sh.G.* (2018). Klassifikatsiya rubezhei dostupa i svyazannykh s nimi faktorov vliyaniya v sisteme kontrolya dostupa [Classification of access points

and related influence factors in the access control system]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*. № 1. pp. 62-70. [in Russian]

Magomedov, 2018 – *Magomedov Sh.G.* (2018). Klassifikatsiya rubezhei dostupa i svyazannykh s nimi faktorov vliyaniya v sisteme kontrolya dustup [Classification of access points and related influence factors in the access control system]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*. № 1. pp. 62-70. [in Russian]

Metody Khuka-Dzhivsa – Metody Khuka-Dzhivsa [Hook-Jeeves methods]. Minsk: Belorusskaya tsifrovaya biblioteka LIBRARY.BY. Data obnovleniya: 04 iyunya 2010. URL: http://library.by/portalus/modules/different/readme.php?subaction=showfull&id=1275677296&archive=1275730016&start_from=&ucat=& (data obrashcheniya: 29.07.2018). [in Russian]

Orlovskii, 1981 – *Orlovskii S.A.* (1981). Problemy prinyatiya reshenii pri nechetkoi iskhodnoi informatsii [Decision problems with fuzzy source information]. M.: Nauka. Gl. red. fiz.-mat. lit. 208 p. [in Russian]

Panov, 2013 – *Panov M.M.* (2013). Otsenka deyatel'nosti i sistema upravleniya kompaniei na osnove KPI [Evaluation of activities and management system of the company based on KPI]. M.: Infra-M. 255 p. [in Russian]

Petrov, 2008 – *Petrov N.V.* (2008). Sistema okhrany perimetra [Perimeter protection system]. *Zashchita informatsii*. Insaid. № 1 (19). pp. 56-61. [in Russian]

Petrov, 2010 – *Petrov N.V.* (2010). Obosnovanie vybora tekhnicheskikh sredstv obnaruzheniya dlya sistem okhrannoi signalizatsii perimetra [Substantiation of the choice of technical detection means for perimeter alarm systems]. *Zashchita informatsii. Insaid*. № 5 (35). pp. 76-86. [in Russian]

Popov, Popova, 2018 – *Popov G.A., Popova E.A.* (2018). Sistemnyi podkhod k formirovaniyu sostava funktsii upravleniya v sistemakh zashchity informatsii [A systematic approach to the formation of the composition of management functions in information security systems]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*. № 1. pp. 71-80. [in Russian]

Rytov i dr., 2015 – *Rytov M.Yu., Eremenko V.T., Gulak M.L.* (2015). Model' protsessa vybora sostava tekhnicheskikh sredstv sistem fizicheskoi zashchity [Model of the process of selecting the composition of technical means of physical protection systems]. *Informatsiya i bezopasnost'*. T. 18. № 4. pp. 502-507. [in Russian]

Shanaev, 2009 – *Shanaev G.* (2009). Inzhenernye sredstva fizicheskoi zashchity perimetra [Engineering means of physical protection of perimeter]. *Algoritm bezopasnosti*. № 4. pp. 6-13. [in Russian]

Shanaev, 2010 – *Shanaev G.* (2010). Varianty postroeniya rubezhei okhrany ob"ekta pri nalichii faktorov, uslozhnyayushchikh funktsionirovanie SZP iskusstvennogo proiskhozhdeniya [Options for constructing boundaries for the protection of the object in the presence of factors complicating the operation of the FFP of an artificial origin]. *Algoritm bezopasnosti*. № 1. pp. 56-60. [in Russian]

Shreider, Borovskii, 2017 – *Shreider M.Yu., Borovskii A.S.* (2017). Primenenie mnogoagentnogo podkhoda k postroeniyu sistem fizicheskoi zashchity ob"ektov [Application of a multi-agent approach to the construction of physical protection systems of objects]. *Intellekt. Innovatsii. Investitsii*. № 10. pp. 66-71.

Simavoryan et al., 2015a – *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*. № 3 (7). pp. 212-220.

Simavoryan et al., 2015b – Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. (2015). Research of the intellectual antagonism of malefactors and service of information security in the ADPS. *Modeling of Artificial Intelligence*. № 1 (5). pp. 33-41.

Simavoryan et al., 2016a – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* (2016). Creating the conditions for the theoretical and practical solution of the problem of automated intelligent search for the attacker's image in ADPS. *Modeling of Artificial Intelligence*. № 3 (11). pp. 166-176.

Simavoryan et al., 2016b – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Samarin V.I., Simonyan R.A., Kardashyan M.A.* (2016). Enhancing operational efficiency of the fuzzy image of the attacker's method of iterations. *Modeling of Artificial Intelligence.* № 4 (12). pp. 187-193.

Simavoryan et al., 2017 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Makarova I.L., Simonyan R.A.* (2017). The task of determining the optimal technological scheme for the operation of information security systems. *European Journal of Computer Science.* № 3 (1). pp. 17-22.

Simavoryan i dr., 2013 – *Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A.* (2013). Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii [A systems approach to the design of intelligent information security systems]. *Izvestiya Sochinskogo gosudarstvennogo universiteta,* № 4-2(28), pp. 128-132. [in Russian]

Simavoryan, 2009a – *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. 1115. [in Russian]

Simavoryan, 2009b – *Simavoryan S.Zh.* (2009). Ponyatie neopredelennosti v zadachakh zashchity informatsii [The concept of uncertainty in problems of information protection. Survey of applied and industrial mathematics]. *Obozrenie prikladnoi i promyshlennoi matematiki.* T. 16. № 6. P. 1115. [in Russian]

Simavoryan, 2010 – Simavoryan S.Zh. (2010). O neobkhodimosti prepodavaniya distsipliny "Informatsionnaya bezopasnost'" na gumanitarnykh fakul'tetakh VUZov [On the need to teach the discipline "Information Security" at the Humanities faculties of universities]. *Vestnik Sochinskogo gosudarstvennogo universiteta turizma i kurortnogo dela.* № 4. pp. 65-73. [in Russian]

Simavoryan, 2011 – *Simavoryan S.Zh.* (2011). About application during lectures on protection of the information and information security of the method of "The round table". *European Researcher.* № 5-1 (7). pp. 760-762.

Smirnov i dr., 2018 – *Smirnov A.V., Khabibulin R.Sh., Tarakanov D.V.* (2018). Primenenie mnogoagentnogo podkhoda dlya podderzhki upravleniya bezopasnost'yu v tekhnosfere [Application of a multi-agent approach to support security management in the technosphere]. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta.* T. 22. № 1. pp. 118–133. DOI: 10.21285/1814-3520-2018-1-118-133 [in Russian]

Standart banka Rossii... – Standart banka Rossii STO BR IBBS-1.0–2014 [Standard of the Bank of Russia SRT BR IBBS-1.0-2014]. Obespechenie informatsionnoi bezopasnosti organizatsionnoi bankovskoi sistemy Rossiiskoi Federatsii. Obshchie polozheniya [Elektronnyi resurs]. URL: http://www.cbr.ru/credit/gubzi_docs/st-10-14.pdf (data obrashcheniya: 08.06.18). [in Russian]

Stefarov, Zhukov, 2012 – *Stefarov A.P., Zhukov V.G.* (2012). Formirovanie tipovoi modeli narushitelya pravil razgranicheniya dostupa v avtomatizirovannykh sistemakh [Formation of a typical model of the violator of the rules of access delimitation in automated systems]. *Izvestiya YuFU. Tekhnicheskie nauki.* № 12 (137). pp. 45-54. [in Russian]

Tarasov, 2010 – *Tarasov A.D.* (2010). Sistema fizicheskoi zashchity na osnove agentno-orientirovannogo podkhoda i nechetkoi logiki [System of physical protection based on agent-based approach and fuzzy logic]. *Problemy upravleniya i modelirovaniya v slozhnykh sistemakh: materialy XII Mezhdunar. konf. (Samara, 21–23 iyunya 2010 g.).* Samara, pp. 650–656. [in Russian]

Tumurov i dr., 2016 – *Tumurov G.V., Voznyuk A.N., Kshnyankin A.P.* (2016). Model' narushitelya podsistemy tekhnicheskoi zashchity informatsii ob"ekta informatizatsii [Model violator of the subsystem of technical protection of information of the object of information]. *Elektronnye sredstva i sistemy upravleniya.* № 1-2. pp. 62-64. [in Russian]

Yannikov i dr., 2017 – *Yannikov I.M., Soboleva N.V., Kudel'kin V.A., Kazantsev M.M., Gabrichidze T.G.* (2017). Baza dannykh sredstv fizicheskoi zashchity potentsial'no opasnykh ob"ektov [Database of means of physical protection of potentially dangerous objects]. *Intellektual'nye sistemy v proizvodstve.* T. 15. № 1. pp. 122-125. [in Russian]

Zubareva i dr., 2016 – *Zubareva M.G., Tsvetkov A.A., Khamush A.L., Shorokh D.K., Shuklin A.V., Yurskov S.V.* (2016). Metodologii proektirovaniya mul'tiagentnykh sistem

[Methodology for the design of multi-agent systems]. *Tekhnicheskie nauki v Rossii i za rubezhom Materialy VI Mezhdunarodnoi nauchnoi konferentsii*. pp. 3-8. [in Russian]

Построение интеллектуальных систем физической защиты информации

Симон Жоржевич Симаворян [a, *], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a], Ирина Леонидовна Макарова [a], Элина Анатольевна Пилосян [a], Рафаэль Арсенович Симонян [b]

[a] Сочинский государственный университет, Российская Федерация

Аннотация. Одной из важнейших задач проектирования интеллектуальных систем защиты информации (ИСЗИ) в автоматизированных системах обработки данных (АСОД) является задача построения интеллектуальных систем физической защиты информации (ИСФЗ). В настоящее время задача построения ИСФЗ является актуальной, требующей системного и регулярного решения на постоянной основе. В настоящее время разработано достаточно много математических моделей и практических подходов решения задачи эффективного функционирования систем физической защиты. Одними из интересных подходов к решению этой задачи являются:1) интегрированный подход по разработке математической модели функционирования систем физической защиты (Боровский, Тарасов, 2011a, Боровский, Тарасов, 2011b; Боровский, Тарасов, 2011b; Боровский, 2016; Годырева и др., 2007); 2) многоагентные системы (МАС) и технологии (МАС-технологии) (Шрейдер, Боровский, 2017; Смирнов и др., 2018; Городецкий и др., 2017; Тарасов, 2010; Зубарева и др., 2016).

Однако, анализ нормативно-методической базы физической безопасности, проведённый в работе (Филиппов, 2017) показывает, что методики категорирования, анализа угроз и уязвимостей отличаются нечеткостью понятийного аппарата и отсутствием единого терминологического подхода. Кроме того, в работе подчёркивается, что при анализе угроз зачастую не рассматривается связь уязвимостей и модели нарушителя. Не составлен банк данных угроз безопасности и актуальных уязвимостей. Однако, следует заметить, что системы физической защиты потенциально опасных объектов во многом зависят от качественного подбора средств физической защиты, и в работе (Янников и др., 2017) предложена, разработанная с помощью MS SQL Server Express база данных «Средства физической защиты потенциально опасных объектов».

Практика показывает, что методология проектирования ИСФЗ разными разработчиками строится на разных методологических основах, что диктуется различной ведомственной принадлежностью АСОД. В соответствии с этим в данной статье сформулирована задача построения интеллектуальных систем физической защиты информации на базе системно-концептуального подхода (Симаворян и др., 2013; Герасименко, Малюк, 1997), проработаны некоторые аспекты её системного решения.

Ключевые слова: физические средства защиты информации, интеллектуальная система защиты информации, системный подход, система физической защиты.

[*] Корреспондирующий автор
Адреса электронной почты: simsim58@mail.ru (С.Ж. Симаворян), oppm@mail.ru (А.Р. Симонян), elenaulitina@mail.ru (Е.И. Улитина), ratton@mail.ru (И.Л. Макарова), azalto@mail.ru (Э.А. Пилосян), raf55@list.ru (Р.А. Симонян)