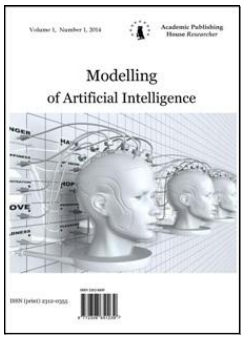

Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
Vol. 5, Is. 1, pp. 33-41, 2015

DOI: 10.13187/mai.2015.5.33
www.ejournal11.com

UDC 004.89

Research of the Intellectual Antagonism of Malefactors and Service of Information Security in the ADPS

[1] Simon Zh. Simavoryan
[2] Arsen R. Simonyan
[3] Elena I. Ulitina
[4] Rafik A. Simonyan

[1]Sochi State University, Russian Federation
354000, Sochi, 26a Sovetskaya St.
PhD (Technical), Associate Professor
E-mail: simsim58@mail.ru
[2]Sochi State University, Russian Federation
354000, Sochi, 26a Sovetskaya St.
PhD (Physics and mathematical), Associate Professor
E-mail: oppm@mail.ru
[3]Sochi State University, Russian Federation
354000, Sochi, 26a Sovetskaya St.
PhD (Physics and mathematical), Associate Professor
E-mail: elenaulitina@mail.ru
[4]Kuban State University, Russian Federation
350040, Krasnodar, Stavropolskaya St., 149
E-mail: raf55@list.ru
Post-graduate student

Abstract

The article describes the main tasks of operational dispatch management of information security in automated data processing systems and analyzed the possibility of using artificial intelligence methods.

Keywords: maintenance control; information protection; methods of artificial intelligence.

Введение

В самом общем виде на чисто прагматическом уровне требования к защите информации в автоматизированных системах обработки информации (АСОД) могут быть определены как закрытие всех потенциально возможных каналов несанкционированного получения информации (КНПИ), или по крайней мере тех из них, проявление которых может привести к несанкционированному получению информации (НПИ). Отличительной особенностью оперативно-диспетчерского управления (ОДУ) является требование краткосрочного управления. В работе [2] предложен системный подход к проектированию интеллектуальных систем защиты информации, поэтому задача ОДУ для интеллектуальных

систем защиты информации становится актуальной и прагматичной. Решение задач ОДУ, во-первых, краткосрочное, во-вторых, зависит от уровня интеллектуализации самой системы защиты информации [3], в-третьих, от уровня интеллектуальности злоумышленника [4]. Противоборство злоумышленников и службы защиты информации [14] требует использования методов из области искусственного интеллекта. Этому и посвящена данная работа.

Материалы и методы

В рамках исследования были проанализированы методы получения и извлечения знаний из области искусственного интеллекта [5]: наблюдения, протоколы «мыслей вслух», лекции, «мозговой штурм», круглый стол, ролевые игры, анкетирование, интервью, диалог, экспертные игры, анализ учебников, анализ литературы, анализ документов.

В работе [4] было подчеркнуто, что современный злоумышленник относится к классу интеллектуальных злоумышленников, поэтому и методы борьбы с ним должны быть интеллектуальными. С учетом вышесказанного, в данной работе была поставлена задача о разработке алгоритма принятия решении по ОДУ защитой информации с использованием методов искусственного интеллекта

Результаты и их обсуждение

Основными макропроцессами управления защитой информации в АСОД являются: оперативно-диспетчерское управление (ОДУ) защитой информации, календарно-плановое руководство, планирование и обеспечение повседневной деятельности службы защиты информации [1].

ОДУ защитой информации – организованное реагирование на непредвиденные ситуации, которые возникают в процессе функционирования управляемых объектов или процессов. Календарно-плановое руководство защитой – регулярный сбор информации о ходе выполнения планов защиты и изменении условий защиты, анализе этой информации и выработке решений о корректировке планов защиты. Планирование защиты - процесс выработки рациональной (оптимальной) программы предстоящей деятельности. В общем случае различают долгосрочное (перспективное), среднесрочное и текущее планирование. Обеспечение повседневной деятельности всех подразделений и отдельных должностных лиц, имеющих непосредственное отношение к защите информации – планирование, организация, оценка текущей деятельности, сбор, накопление и обработка информации, относящейся к защите, принятие текущих решений и др.

Сформулируем основные задачи ОДУ интеллектуальной защитой информации в АСОД:

- Задача Z1. Непрерывный интеллектуальный анализ и распознавание ситуаций, связанных с проявлением каналов НПИ во всех зонах защиты информации АСОД;
- Задача Z2. Сбор, обработка и формирование интеллектуальных баз данных по защите информации;
- Задача Z3. Контроль и анализ адекватности выполнения задач защиты информации в соответствии с функциями защиты информации;
- Задача Z4. Контроль и анализ надежности функционирования средств защиты информации в соответствии с задачами защиты информации;
- Задача Z5. Интеллектуальный анализ и прогнозирование развития ситуаций, связанных с НПИ;
- Задача Z6. Принятие решений по оперативному и практическому контролю доступа злоумышленников в зону защиты информации, с возможностью, в случае необходимости, вмешательства в работу подсистемы доступа злоумышленников в зону защиты информации;
- Задача Z7. Принятие решений по оперативному и практическому контролю наличия КНПИ в зоне защиты информации, с возможностью, в случае необходимости, вмешательства в работу подсистемы контроля наличия КНПИ в зонах защиты информации;
- Задача Z8. 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 Z9. Принятие решений по оперативной и практической локализации НПИ, с возможностью, в случае необходимости, вмешательства в работу подсистемы локализации НПИ;

- Задача Z10. Принятие решений по оперативной и практической ликвидации последствий НПИ, с возможностью, в случае необходимости, вмешательства в работу подсистемы ликвидации последствий НПИ;

- Задача Z11. Внесение и корректировка разработанных предложений по внесению изменений в планы по ОДУ защитой информации;

- Задача Z12. Отработка учетно-отчетных документов, относящихся к оперативно-диспетчерскому защитой информации.

Общая структура алгоритма оперативно-диспетчерского управления защитой информации приводится на рисунке 1.

Задача Z1 в классической формулировке может быть отнесена к задачам распознавания образов, которые к настоящему времени исследованы и разработаны достаточно [9]. Несмотря на это, методы распознавания образов в том виде в каком они есть не могут быть адекватно применены к задачам по выявлению потенциально возможных КНПИ. Причины следующие: во-первых, для каждого защищаемого объекта АСОД необходимо сформировать полное структурированное множество потенциально возможных ситуаций (распознаваемых образов); во-вторых, определить перечень тех признаков, по которым можно охарактеризовать реальную ситуацию как опасную; в-третьих, выбрать методику, по которой можно определить вероятностные (количественные) характеристики уязвимости информации, т.е. посчитать вероятности: 1) доступа злоумышленника в зону защиты; 2) наличия каналов НПИ в зоне защиты; 3) наличия информации в канале в момент доступа злоумышленника к каналу; 4) локализации НПИ; 5) ликвидации последствий НПИ [11, 12, 13]. Задача определения вероятностных показателей защищенности информации при большом числе взаимосвязанных событий представляет собой достаточно сложную задачу. Эта задача относится к классу задач прогнозирования случайных процессов.

Задача Z2 заключается в том, что для решения этой задачи необходимо создание интеллектуальной базы знаний по защите информации. Такая база знаний может быть построена на основе построения информационного кадастра по методологии, изложенной в работе [6] и требует дальнейшей разработки.

Задача Z3 заключается в схемном отслеживании выполнения задач защиты информации в соответствии с регламентом их временного выполнения. Выполнение этой задачи требует наличия каталога КНПИ и каталога задач защиты информации.

Задача Z4 заключается в схемном отслеживании использования средств защиты информации при решении соответствующих задач защиты информации в соответствии с регламентом их временного выполнения. Выполнение этой задачи требует наличия каталога задач защиты информации и каталога средств защиты информации.

Задача Z5 заключается в том, что необходимо оперативно выявлять и распознавать ситуации выходящие из-под контроля. При этом под сущностью прогнозирования развития ситуаций понимаются все приемлемые и возможные варианты действий злоумышленников с целью НПИ.

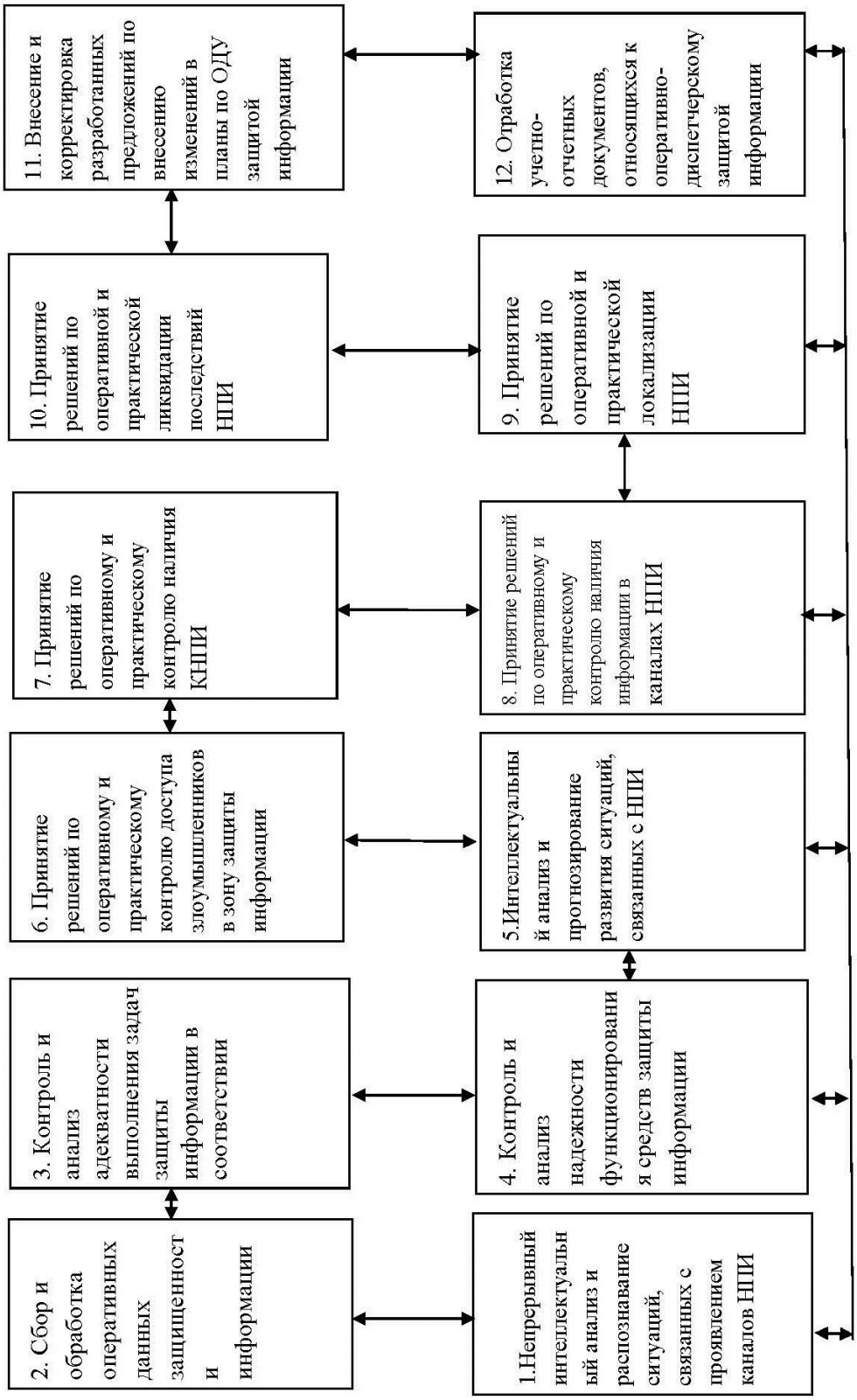

Рис. 1. Общая структура алгоритма оперативно-диспетчерского управления

Задача Z6 заключается в оперативном вмешательстве в процесс контроля доступа злоумышленников в зону защиты информации. С целью оперативного реагирования на несанкционированный доступ злоумышленников в зону защиты информации целесообразно на рабочих местах сотрудников службы безопасности иметь стенд, т. е. схему действий. Форма и содержание такого стенда (вариант) приводится в [1]. При этом для должностных лиц необходимо сделать инструкции по реагированию на ситуацию, например, проверить достоверность имеющихся данных характеризующих ситуацию; принять неотложные меры по спасению людей и материальных ценностей; принять меры по пресечению злоумышленных действий и задержанию нарушителя; принять меры по локализации НПИ; доложить руководству о ситуации и принятых мерах; принять меры по ликвидации последствий НПИ.

Задачи Z7, Z8, Z9, Z10 по содержанию и требованиям аналогичны задаче Z6 с учетом своих особенностей и требуют дополнительных разработок.

Задача Z11 внесения и корректировки разработанных предложений по внесению изменений в планы ОДУ защитой информации является обычной оптимизационной задачей, решение которой являются общеизвестно и не представляет трудности [1, 10].

Задача Z12 отработки учетно-отчетных документов, относящихся к оперативно-диспетчерскому управлению защитой информации, является стандартной информационной задачей, методология решения таких задач к настоящему времени рассмотрена достаточно полно и детально [10].

На решение задач ОДУ значительно оказывают влияние ситуации, связанные с неясностью или неопределенностью проявления каналов НПИ [1, 8]. В [1] для выхода из таких ситуаций используется сеанс анализа ситуации по эвристической программе. Сеанс проводится в виде диалога ведущего с решающим. Исходя из того, что при ОДУ времени на решение задач, как правило, выделяется мало, то при проведении сеанса необходимо формулировать вопросы надо так, чтобы по возможности исключалась неоднозначность и противоречивость их трактовок. Это позволяет не привлекать дополнительно к сеансу экспертов для принятия решений, т. е. служба защиты должна принимать решения самостоятельно своими силами. Но это, в свою очередь, предъявляет повышенные требования к основным действующим лицам, т.е. к ведущему и решающему.

Наибольшая степень неопределенности будет иметь место при анализе нестандартных ситуаций. В этих условиях для обоснованного принятия решения целесообразно производить детальный и пошаговый анализ сложившейся ситуации, связанных с проявлениями КНПИ и возможных направлений развития злоумышленных действий [8]. Поэтому следует провести анализ возможностей применение известных методов принятия решений из области искусственного интеллекта, например, таких как методы получения и извлечения знаний.

Для анализа возможностей применения методов получения и извлечения знаний при решении задач ОДУ введем следующие обозначения: M1 – метод наблюдения, M2 – метод протокол «мыслей вслух», M3 – метод лекции, M4 – метод «мозгового штурма», M5 – метод круглого стола, M6 – метод ролевых игр, M7 – метод анкетирования, M8 – метод интервью, M9 – метод диалога, M10 – метод экспертные игры, M11 – метод анализа учебников, M12 – метод анализа литературы, M13 – метод анализа документов [5].

Возможности применения методов получения и извлечения знаний применительно к задачам ОДУ приводятся в таблице 1, где знак «+» означает – возможность применения данного метода к решению данной задачи, и знак «-» означает – нецелесообразность применения данного метода для решения данной задачи.

Таблица 1. Использование методов ИИ при решении задач ОДУ

Методы ИИ / ОДУ Задачи	M1	M2	M3	M4	M5	M6	M7	M8	M9	M 10	M 11	M 12	M 13
Z1	+	+	-	+	+	-	-	-	+	-	-	-	+
Z2	+	+	-	+	+	-	-	-	+	-	-	-	+
Z3	+	+	-	+	+	-	-	-	+	-	-	-	+
Z4	+	+	-	+	+	-	-	-	+	-	-	-	+
Z5	+	+	-	+	+	-	-	-	+	-	-	-	+
Z6	+	+	-	+	+	-	-	-	+	-	-	-	+
Z7	+	+	-	+	+	-	-	-	+	-	-	-	+
Z8	+	+	-	+	+	-	-	-	+	-	-	-	+
Z9	+	+	-	+	+	-	-	-	+	-	-	-	+
Z10	+	+	-	+	+	-	-	-	+	-	-	-	+
Z11	+	+	-	+	+	-	-	-	+	-	-	-	+
Z12	+	+	-	+	+	-	-	-	+	-	-	-	+

Таким образом, анализ таблицы 1 показывает, что при ОДУ применимы следующие методы: наблюдения, протокол «мыслей вслух», мозгового штурма, круглого стола, диалога, анализа документов. Описания данных методов можно найти в [5].

Важную роль в ОДУ защитой информации играет повышение уровня квалификации сотрудников службы безопасности. При анализе возможностей применения методов получения и извлечения знаний видно, что такие методы как: лекция, ролевые игры, анкетирование, интервью, экспертные игры, анализ учебников и анализ литературы не применимы в ходе ОДУ из-за ограниченности времени выделенного на принятие решений по оперативному закрытию канала НПИ. Но нами сделан вывод о необходимости применения этих методов вне процесса ОДУ, как методов обучения сотрудников службы защиты информации и как методов разработки оперативно-плановых мероприятий. Например, в работе [7] приводится возможности применения во время лекций метода круглого стола.

ОДУ защитой информации характеризуется принятием персоналом службы защиты информации решений в реально складывающейся или сложившейся ситуацией, которая может привести к утечке информации. В этих условиях разработанные оперативно-диспетчерские задания или решения руководителей подразделений службы защиты информации должны обеспечить строгий и четкий во времени контроль выполнения всех запланированных регламентных работ. Этому соответствует разработка графиков проверки адекватности выполнения задач защиты информации, надежности функционирования средств защиты информации и сменно-суточных заданий на подразделения и рабочие места службы защиты.

Таким образом, ОДУ осуществляется на основе непрерывного (повседневного) слежения за ходом работы службы защиты информации, оказывая целенаправленное воздействие на сотрудников службы защиты информации по безусловному выполнению всех утвержденных производственных программ. Это достигается: строгим распределением работ на короткие периоды времени; четкой организацией сбора и обработки информации о проявлении каналов НПИ; комплексным решением задач защиты информации; комплексным использованием средств защиты информации; повседневным анализом и владением персоналом ситуацией, связанной с утечкой информации; своевременным

принятием решений и организацией работы по предупреждению нарушений в ходе выполняемых работ; своевременным принятием решений при локализации НПИ; своевременным принятием решений при ликвидации последствий НПИ. регулирующих воздействий на ход процесса защиты информации. Составление оперативно-календарного плана - сложная, трудоемкая работа, требующая предварительного глубокого анализа реальных условий месторасположения АСОД, выявления характерных особенностей всех зон защиты, условий и требований к защите информации. Поэтому здесь мы имеем дело с особенностями проявления каналов НПИ применительно к каждой зоне защиты информации. Разработка сменно-суточного задания является заключительным этапом оперативно-диспетчерского обеспечения защитой информации. Оно конкретизирует на очередные сутки (по сменам) задания оперативно-календарного плана по закрытию каналов НПИ с учетом: непредвиденного выхода из строя средств защиты информации; непредвиденного недовыполнения задачи защиты информации; невыходов на работу сотрудников службы защиты информации.

Заключение

Из вышесказанного, нетрудно видеть, что применение методов получения и извлечения знаний способствует повышению не только уровня организации ОДУ, но и уровня эффективного управления защитой информации в вычислительных системах и сетях в целом.

Благодарности

Работа поддержана грантом РФФИ 13-01-00544.

Примечания:

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997. 540 с.
2. 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.
3. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one Approach to a Question of Classification of Intellectual System of Information Security// Modeling of Artificial Intelligence, 2014, Vol (1), № 1, p. 29-44.
4. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД // Известия Сочинского государственного университета, 2014, № 4-1 (32), с. 15-23.
5. Гаврилов Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем. СПб.: Издательский дом «Питер», 2001. 384 с.
6. Герасименко В.А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. 320 с.
7. Симаворян С.Ж. О применении во время лекций по защите информации и информационной безопасности метода «Круглого стола» // European researcher, 2011, №5-1 (7), pp. 760-762.
8. Симаворян, С. Ж. Понятие неопределенности в задачах защиты информации // Обозрение прикладной и промышленной математики / Под ред. Ю. В. Прохорова. М.: Редакция журнала «ОПиПМ». 2009. Том 16, выпуск 6. С. 1115.
9. Симаков В.С., Луценко Е.В. Адаптивное управление сложными системами на основе теории распознавания образов. Краснодар, КГТУ. 1999. 318 с.
10. Аверченков В.И. Аудит информационной безопасности. М.: ФЛИНТА, 2011. 269 с.
11. Симаворян С. Ж. Применение методов Data Mining для обнаружения инсайдеров // Обозрение прикладной и промышленной математики / Под ред. Ю. В. Прохорова. М.: Редакция журнала «ОПиПМ». 2010. Том 17, выпуск 3. С. 455-456.
12. Simon Zh. Simavoryan, Arsen R. Simonyan. The Probabilistic Safety Assessment Model of Anti-Terrorist Security of Olimpic games // Europen Reserсher. 2012. Vol(20). № 5-1, p. 532-536.
13. Симаворян С. Ж. Аналитическая модель определения показателя уязвимости информации в автоматизированных системах обработки информации (АСОД) // Обозрение

прикладной и промышленной математики / Под ред. Ю. В. Прохорова. – М.: Редакция журнала «ОПиПМ». 2009. Том 16, выпуск 6. С. 1114.

14. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД // Известия Сочинского государственного университета, 2014, № 4-1 (32). С 15-23.

References:

1. Gerasimenko V.A., Malyuk A.A. Osnovy zashchity informatsii. M., 1997. 540 s.
2. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. Sistemnyi podkhod k proektirovaniyu intellektual'nykh sistem zashchity informatsii. // «Izvestiya Sochinskogo gosudarstvennogo universiteta», 2013, № 4-2(28), s. 128-132.
3. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan R.A. About one Approach to a Question of Classification of Intellectual System of Information Security// Modeling of Artificial Intelligence, 2014, Vol (1), № 1, p. 29-44.
4. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD // Izvestiya Sochinskogo gosudarstvennogo universiteta, 2014, № 4-1 (32). С 15-23.
5. Gavrilov T.A., Khoroshevskii V.F. Bazy znanii intellektual'nykh sistem. – SPb: Izdatel'skii dom «Piter», 2001. – 384 s.
6. Gerasimenko V.A. Osnovy informatsionnoi gramoty. - M.: Energoatomizdat, 1996. – 320 s.
7. Simavoryan S.Zh. O primenenii vo vremya lektsii po zashchite informatsii i informatsionnoi bezopasnosti metoda «Kruglogo stola» // «European researcher» (Evropeiskii issledovatel'), 2011, №5-1 (7), s. 760-762.
8. Simavoryan, S. Zh. Ponyatie neopredelennosti v zadachakh zashchity informatsii // Obozrenie prikladnoi i promyshlennoi matematiki / Pod red. Yu. V. Prokhorova. – M.: Redaktsiya zhurnala «OPiPM». 2009. Tom 16, vypusk 6. S. 1115.
9. Simakov V.S., Lutsenko E.V. Adaptivnoe upravlenie slozhnymi sistemami na osnove teorii raspoznavaniya obrazov. Krasnodar, KGTU. 1999. 318 s.
10. Averchenkov V.I. Audit informatsionnoi bezopasnosti. M.: FLINTA, 2011. 269 s.
11. Simavoryan, S. Zh. Primenenie metodov Data Mining dlya obnaruzheniya insaiderov // Obozrenie prikladnoi i promyshlennoi matematiki / Pod red. Yu. V. Prokhorova. M.: Redaktsiya zhurnala «OPiPM». 2010. Tom 17, vypusk 3. S. 455-456.
12. Simon Zh. Simavoryan, Arsen R. Simonyan. The Probabilistic Safety Assessment Model of Anti-Terrorist Security of Olimpic games. Europen Resercher. 2012. Vol(20). № 5-1. R. 532-536.
13. Simavoryan S. Zh. Analiticheskaya model' opredeleniya pokazatelya uyazvimosti informatsii v avtomatizirovannykh sistemakh obrabotki informatsii (ASOD) // Obozrenie prikladnoi i promyshlennoi matematiki / Pod red. Yu. V. Prokhorova. M.: Redaktsiya zhurnala «OPiPM». 2009. Tom 16, vypusk 6. S. 1114.
14. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD // Izvestiya Sochinskogo gosudarstvennogo universiteta, 2014, № 4-1 (32). С 15-23.

УДК 004.89

Разработка алгоритма принятия решений по оперативно-диспетчерскому управлению средствами защиты информации на основе методов искусственного интеллекта

[1] Симон Жоржевич Симаворян
[2] Арсен Рафикович Симонян
[3] Улитина Елена Ивановна
[4] Рафик Арсенович Симонян

[1] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
кандидат технических наук, доцент
E-mail: simsim58@mail.ru
[2] Сочинский государственный университет, Россия
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
кандидат физ-мат. наук, доцент, доцент
E-mail: oppm@mail.ru
[3] Сочинский государственный университет, Россия
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
кандидат физ-мат. наук, доцент
E-mail: ulitinaelena@mail.ru
[4] Кубанский государственный университет, Российская Федерация
350040, г. Краснодар, ул. Ставропольская, 149
аспирант
E-mail: raf55@list.ru

Аннотация. В статье рассмотрены основные задачи оперативно-диспетчерского управления защитой информации в автоматизированных системах обработки данных и проанализированы возможности использования методов искусственного интеллекта.

Ключевые слова: оперативно-диспетчерское управление; защита информации; методы искусственного интеллекта.