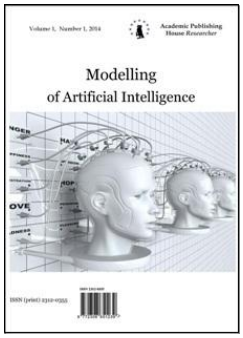

Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
Vol. 1, No. 1, pp. 29-44, 2014

DOI: 10.13187/issn.2312-0355
www.ejournal11.com

UDC 004.89

About one Approach to a Question of Classification of Intellectual Systems of Information Security*

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

[1-2] Sochi State University, Russian Federation
Sovietskaya st., 26a, Sochi city, Krasnodar Krai, 354000
[1] PhD (Technical), associate professor
E-mail: simsim58@mail.ru
[2] PhD (Physics and mathematical), associate professor
E-mail: oppm@mail.ru
[3] PhD (Physics and mathematical), associate professor
E-mail: elenaulitina@mail.ru
[4]Kuban State University, Russian Federation
Stavropolskaya st., 149, Krasnodar, 350040
E-mail: raf55@list.ru
post-graduate students

Abstract. In article the literature analysis concerning determination of intellectuality of systems of information security is made. As a result of the analysis the conclusion expansion of concept of intellectuality of systems of information security is drawn. New classification which gives a view of this problem much more widely is given.

Keywords: intellectual systems of information security, intellectuality levels.

Введение.

В настоящее время в области информационной безопасности автоматизированных систем обработки данных (АСОД) особое внимание уделяется вопросу проектирования интеллектуальных систем защиты информации (ИСЗИ). Одним из существенных факторов характеризующих ИСЗИ является степень (уровень) интеллектуальности систем защиты информации. В существующей литературе делались и делаются попытки определения понятия интеллектуальности систем защиты информации. Некоторые полученные результаты в области искусственного интеллекта представляют собой как теоретический, так и практический интерес. Наиболее интересные и существенные результаты, с точки зрения их адаптации к системам защиты информации приведены в работах [1, 2]. Однако, анализ публикаций в этой области и полученные результаты не дают должного представления о полноте или значимости решаемых задач по проектированию ИСЗИ.

* Работа поддержана грантом РФФИ 13-01-00544.

Поэтому авторами этой статьи предложен подход, который системно определяет понятие уровня интеллектуальности систем защиты информации.

Материалы и методы.

В работе использованы публикации из области проектирования систем защиты информации, а также искусственного интеллекта.

Обсуждение.

В области развития искусственного интеллекта можно выделить следующие традиционные направления: 1) Распознавание образов; 2) Доказательство теорем и решение задач; 3) Игры и принятие решений; 4) Естественные языки и их машинное понимание. Машинный перевод; 5) «Разумные роботы»; 6) Экспертные системы. 7) Моделирование творческой деятельности; 8) Моделирование нейронных сетей. Моделирование поведения животных; 9) Специализированные интеллектуальные системы промышленного, военного, космического и т.п. назначения [1].

В работе [1] проведен всесторонний философский анализ проблемы возможности создания «интегрального» искусственного интеллекта, т. е. создания искусственных систем, эквивалентных по своим функциональным, поведенческим возможностям человеческому интеллекту. Дано четкое определение понятий «интеллект» и «искусственный интеллект». Объектом исследования выступает «искусственный интеллект», рассматриваемый как совокупность технических средств, моделирующих различные аспекты «естественного» интеллекта человека. Предметом исследования выступает проблема принципиальной возможности создания искусственного интеллекта, тождественного по своим функциональным возможностям естественному. В работе впервые продемонстрировано принципиальное различие в понимании сущности интеллекта и искусственного интеллекта в философии и в компьютерных науках. Показано, что функционалистский подход, исследуя естественный интеллект с позиций компьютерных наук, интерпретирует мыслительную способность человека, как реализацию алгоритмического вычисления, не принимая во внимание сложности и парадоксы, к которым ведет идея полной алгоритмизации мыслительных процессов. Получен вывод, что теоретические разработки в области «интегрального» искусственного интеллекта, несмотря на многочисленные успехи в области практического создания конкретных (локальных) интеллектуальных систем, свидетельствуют о принципиальных трудностях на пути создания полноценного искусственного аналога человеческого интеллекта, отвечающего сформированным в философии представлениям о человеческой интеллектуальности.

Основные положения сформулированные в работе следующие:

1. Интеллект представляет собой целостный комплекс способностей, включающий здравый смысл, рассудок, разум и интуицию. Наличие интеллекта предполагает способность к теоретическому обобщению, к творческому мышлению, предполагает способность не только самостоятельно решать задачи, но и самостоятельно их ставить, открывать новые проблемные области исследования.

2. В современных философских и научных исследованиях по искусственному интеллекту последний понимается как способность решать интеллектуальные задачи путем приобретения, запоминания и целенаправленного преобразования знаний в процессе обучения, а также при адаптации к разнообразным обстоятельствам. Понятие интеллектуальности как способности к решению определенных задач не отражает всей многомерности и сложности человеческой интеллектуальной деятельности. Важнейшая характеристика человеческого интеллекта – способность не только решать, но и ставить принципиально новые задачи – не поддается алгоритмической имитации.

3. Практические трудности создания интегрального искусственного интеллекта определяются принципиальными качественными отличиями человеческого интеллекта от алгоритмических систем. В пользу существования таких качественных отличий свидетельствует ряд аргументов философского и логико-математического характера («геделевский аргумент», «аргумент китайской комнаты» и др.), которые показывают, что человеческий интеллект обладает способностями (ассоциируемыми с понятием «творчество»), выходящими за рамки возможностей любых, сколь угодно сложных

алгоритмических систем. Сказанное, однако, не исключает возможности алгоритмического воспроизведения отдельных, не носящих явно творческого характера интеллектуальных функций или интеллектуальной деятельности человека в конкретных предметных сферах (шахматы, решение логических задач заданного уровня сложности, управление конкретным производством).

4. Натуралистические подходы к пониманию природы сознания и решению психофизической проблемы, наиболее соответствующие идее о возможности алгоритмической имитации человеческого интеллекта (элиминирующие теории и функциональный подход), неудовлетворительны в концептуальном плане, поскольку либо вообще отрицают наличие сознания, либо не способны объяснить, как явления сознания (как феномены внутреннего мира) могут возникнуть в качестве «результата мозговой деятельности». Другие (ненатуралистические) подходы к решению психофизической проблемы: двухаспектный подход (психофизический параллелизм) и дуализм (интеракционизм) явно не совместимы с идеей возможности создания искусственного интеллекта.

5. Всякая аргументация, основанная на экспериментах в области возможности создания искусственного интеллекта, должна быть подвергнута строгому анализу на теоретико-философском уровне, вне которого любые утверждения о возможности создания искусственного интеллекта или о его успешном моделировании как свершившемся факте не могут быть признаны истинными.

Выводы сделанные в работе [1] могут также расширить понимание проблем создания интеллектуальных систем в различных областях науки и техники, в частности в области создания интеллектуальных систем защиты информации.

В работе [2] Дубинский А.Г. предлагает свой взгляд на проблему научного обоснования терминологии в области искусственного интеллекта, даёт определение интеллекта как способности решать «задачи». Автор рассматривает меру изменчивости, динамику, пути развития интеллекта, уровни интеллекта и возможность применения определения понятия «интеллект». Причем величина интеллекта зависит от выбора классов задач. В понятие «Задачи» входят в первую очередь такие классы проблемных ситуаций, когда необходимо осуществить: сбор информации, оценку ситуации, принятие решений, осуществление действий. К группе наиболее важных классов «задач» относятся: формулировка целей, постановка задач, построение моделей, выдвижение гипотез, оценка достоверности решений, верификация моделей, декомпозиция задач, упрощение, планирование, классификация/категоризация, выбор из многих альтернатив, распознавание образов, и проч.

Интеллект – это способность самостоятельно, эффективно (верно, с возможно меньшими затратами ресурсов) находить качественные (верные, простые, требующие как можно меньших затрат ресурсов) решения (в том численовые, ранее неизвестные) разнообразных сложных «задач», в том числе новых, ранее неизвестных (в идеале – любых возможных «задач»). Интеллект характеризуется уровнем и величиной (величинами).

Величина – это количественная мера. Интеллект на разных уровнях отличается качественно. Наличие интеллекта определенного уровня подразумевает наличие интеллекта всех нижележащих уровней (безотносительно к их величинам).

В работе [2] рассмотрены 4 уровня интеллекта.

Интеллект уровня 0 - это способность объекта решать известные «задачи» известными, неизменными методами. Характеризуется скоростью нахождения решений и качеством известных методов (решений). Может быть описан числом – коэффициентом интеллекта (IQ).

Примеры: инстинкт, программа, алгоритм, прошивка ПЗУ.

Сложность построения искусственного интеллекта (ИИ) уровня 0 определяется только сложностью целевого класса задач. Системы ИИ уровня 0 для классов простых задач обычно не считаются интеллектуальными.

Интеллект уровня 1 - это способность объекта улучшать, оптимизировать известные решения задач известных классов. Это способность обучаться, совершенствоваться эволюционным путем. Характеризуется обучаемостью – скоростью обучения и эффективностью – количественным увеличением величины интеллекта уровня 0. Прямые измерения величины интеллекта уровня 1 затруднены.

Примеры: адаптация живых организмов; генетические алгоритмы.

Рассмотрение класса задач оптимизации приводит к возможности эмуляции интеллекта уровня 1 системами с интеллектом уровня 0. Пример: программные пакеты, решающие задачи оптимизации математического программирования.

Системы ИИ уровня 1 обычно называют интеллектуальными.

Интеллект уровня 2 – это способность объекта находить **новые** решения задач известных классов. Его реализация во многом зависит от внешних условий, от того, существуют ли, в принципе, новые, более эффективные решения этих классов задач. Находит себе новые применения по мере возрастания величины интеллекта уровня 0. Трудноизмерим. Возможны численные описания через частоту его применения и эффективность (насколько новые решения лучше известных). Представляет собой революционный путь совершенствования.

Близкие понятия: креативность, относительная новизна, изобретательность.

Интеллект уровня 2 иногда проявляется у высших животных при решении простых задач. При решении сложных классов задач проявляется далеко не у всех людей.

Интеллект уровня 3 – это способность объекта находить (создавать) решения для ранее неизвестных классов задач. Способность решать любые новые задачи. Важнейшая составляющая – это способность к обнаружению новых задач и формулировки их условий. Трудноизмерим. Возможно описание через измерение новизны классов задач (необходим учет топологии и метрики пространства классов задач).

Наличие интеллекта уровня 3 есть безграничность интеллекта, потенциальная бесконечность возможных классов разрешимых задач, потенциальная бесконечность самосовершенствования объекта. Дополнительное качественное отличие: если для предыдущих уровней все сводилось к увеличению интеллекта уровня 0, то для интеллекта уровня 3 это маловажно. Освоение новых классов задач на много порядков лучше (эффективнее, ценнее, выгоднее, интереснее…), чем совершенствование способностей по решению старых задач. Объект с интеллектом уровня 3 может существенно уступать каким-либо другим объектам с интеллектом уровня 0 на каком-либо (или даже на любом) отдельном классе известных задач.

Близкие понятия: абсолютная новизна, научное открытие, изобретение, гениальность.

Следует полагать, что системы ИИ уровня 3 не могут быть разработаны в обозримом будущем и этот уровень интеллектуальной деятельности достижим только для человека, точнее, для лучших (гениальных) представителей человечества.

Интеллект необходим для функционирования в сложной среде, для достижения объектом своих целей (в первую очередь для гомеостаза, выживания, продолжение рода).

Интеллект не требует наличия сознания. Сознание – это производная интеллекта. Можно считать, что интеллект заключен (и) в бессознательном.

Общепринятая концепция обучения требует от учащихся наличия интеллекта лишь 0-го и отчасти 1-го уровня. Современная система среднего и де-факто, высшего образования направлена на развитие только 0-го уровня интеллекта.

Важнейшей задачей человечества является переориентация обучения на развитие 2-го и 3-го уровня интеллекта.

Таким образом, адаптируя данные определения интеллектуальности и уровней интеллекта систем искусственного интеллекта применительно к системам защиты информации, авторами настоящей статьи сделан вывод о необходимости новой классификации интеллектуальных систем защиты информации в АСОД. Нами предлагается системный подход к решению данного вопроса. Для решения данного вопроса нами выбрана следующая последовательность её решения:

1. Определение признаков классификации интеллектуальности систем защиты информации.
2. Классификация систем защиты информации по выбранным признакам интеллектуальности.

Введем следующие определения.

Определение 1. Множество потенциально возможных КНПИ является интеллектуальным, если элементы этого множества удовлетворяют следующим требованиям:

1. Множество КНПИ динамически меняется во времени.

2. Проявление КНПИ зависит от не только от эффективности функционирования средств защиты информации в АСОД, но и от действий злоумышленников, постоянно совершенствующих свои методы и средства вторжения в защищаемую систему.

Определение 2. Множество задач защиты информации является интеллектуальным если:

1. Множество задач защиты информации меняется во времени.
2. Система защиты информации сама ищет новые решения существующих задач защиты информации.
3. Система защиты информации сама генерирует новые задачи или алгоритмы по закрытию потенциально возможных КНПИ.

Определение 3. Множество средств защиты информации является интеллектуальным если:

1. Множество средств защиты информации меняется во времени.
2. Средства защиты информации являются интеллектуальными.

Классификация уровней интеллектуальности систем защиты информации производится по трем признакам: по множеству потенциально возможных КНПИ, по множеству решаемых задач защиты информации и по множеству средств защиты информации. Каждое из этих множеств может быть как заданным, так и интеллектуальным. Тогда в результате такого подхода нами было получено 8 уровней интеллектуальности систем защиты информации.

Уровень 0 - определяется с помощью тройки $\{К_з, З_з, С_з\}$, где $К_з$ - заданное множество потенциально возможных КНПИ, $З_з$ - заданное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации.

Уровень 1- определяется тройкой $\{К_з, З_з, С_и\}$, где $К_з$ - заданное множество потенциально возможных КНПИ, $З_з$ – заданное множество задач защиты информации, $С_и$ – интеллектуальное множество средств защиты информации.

Уровень 2 определяется тройкой $\{К_з, З_и, С_з\}$, где $К_з$ - заданное множество потенциально возможных КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации.

Уровень 3 определяется тройкой $\{К_з, З_и, С_и\}$ - где $К_з$ - заданное множество потенциально возможных КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации.

Уровень 4 определяется тройкой $\{К_и, З_з, С_з\}$, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_з$ – заданное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации.

Уровень 5 определяется тройкой $\{К_и, З_з, С_и\}$, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_з$ - заданное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации.

Уровень 6 определяется тройкой $\{К_и, З_и, С_з\}$, где $К_и$ - интеллектуальное множество КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации.

Уровень 7 (высший уровень) определяется тройкой $\{К_и, З_и, С_и\}$, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_и$ -интеллектуальное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации.

Проведем анализ сформулированных уровней защиты информации в АСОД.

Интеллект уровня 0 – это способность системы защиты информации решать следующие задачи: 1) закрывать заданное множество потенциально возможных КНПИ решением с помощью выбранных задач защиты информации из заданного множества, и 2) решать заданное множество задач защиты информации с помощью выбранных средств защиты информации. Уровень 0 характеризуется эффективностью нахождения решений. Под эффективностью понимается достижение (обеспечение) требуемой защищенности объекта. Системы уровня 0 решают задачи оптимизационного характера, поэтому этот уровень обычно не считают интеллектуальным

Таким образом, система защиты информации обладающая уровнем интеллекта 0 – это система способная решать следующие задачи [3]:

1) выбора задач защиты информации для закрытия заданного множества КНПИ с заданной эффективностью;

2) выбора средств защиты информации для решения заданного множества задач защиты информации с заданной эффективностью.

Решение перечисленных задач приведено в работе [3].

Система защиты информации обладающая уровнем интеллекта 1 – система способная решать следующие задачи:

1) выбора задач защиты информации для закрытия заданного множества КНПИ с заданной эффективностью;

2) выбора интеллектуальных средств защиты информации для решения заданного множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 2 – система способная решать следующие задачи:

1) выбора интеллектуального задач защиты информации для закрытия заданного множества КНПИ с заданной эффективностью;

2) выбора заданных средств защиты информации для решения интеллектуального множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 3 – система способная решать следующие задачи:

1) выбора интеллектуального задач защиты информации для закрытия заданного множества КНПИ с заданной эффективностью;

2) выбора интеллектуальных средств защиты информации для решения интеллектуального множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 4 – система способная решать следующие задачи:

1) выбора заданного множества задач защиты информации для закрытия интеллектуального множества КНПИ с заданной эффективностью;

2) выбора заданных средств защиты информации для решения заданного множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 5 – система способная решать следующие задачи:

1) выбора заданного множества задач защиты информации для закрытия интеллектуального множества КНПИ с заданной эффективностью;

2) выбора интеллектуального множества средств защиты информации для решения заданного множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 6 – система способная решать следующие задачи:

1) выбора интеллектуального множества задач защиты информации для закрытия интеллектуального множества КНПИ с заданной эффективностью;

2) выбора заданного множества средств защиты информации для решения интеллектуального множества задач защиты информации с заданной эффективностью.

Система защиты информации обладающая уровнем интеллекта 7 (высший уровень интеллекта) – система способная решать следующие задачи:

1) выбора интеллектуального множества задач защиты информации для закрытия интеллектуального множества КНПИ с заданной эффективностью;

2) выбора интеллектуального множества средств защиты информации для решения интеллектуального множества задач защиты информации с заданной эффективностью.

В существующей классификации средств защиты информации [3, 4], средства делятся на аппаратные, физические, программные, криптографические, нормативно-правовые акты и морально-этические нормы. Анализ литературы по интеллектуальным средствам защиты информации показывает, что нет четкой классификации интеллектуальных средств защиты информации. А есть перечень изобретенных/разработанных интеллектуальных средств защиты информации для решения определенных задач защиты информации. Следовательно, придерживаясь приведенной классификации следует ее расширить с точки зрения интеллекта. Тогда интеллектуальные средства защиты информации по аналогии следует классифицировать следующим образом: интеллектуальные аппаратные средства защиты информации, интеллектуальные физические средства защиты информации, интеллектуальные программные средства защиты информации, интеллектуальные

криптографические средства защиты информации, законодательные средства защиты интеллектуальной собственности, интеллектуальные морально-этические нормы.

По аналогии с существующей классификацией задач защиты информации [3, 4] можно интеллектуальные задачи защиты информации классифицировать как: интеллектуальные задачи идентификации и аутентификации, интеллектуальные задачи контроля доступа, интеллектуальные задачи маскировки, интеллектуальные задачи регулирования доступа, интеллектуальные задачи регистрации, интеллектуальные задачи уничтожения информации, интеллектуальные задачи сигнализации, интеллектуальные задачи реагирования.

Анализ современной литературы по созданию интеллектуальных систем защиты информации показывает, что в публикациях нет четкой классификации интеллектуальных систем защиты информации, поэтому для анализа уровней интеллекта 1-7, сформулированных в данной работе, авторам предпринята попытка информативного анализа содержания литературы.

В работе [5] показано, что в основном интеллектуальные средства защиты информации нашли свое применение в системах обнаружения атак в качестве интеллектуального инструмента, в которых, как правило, используются нейронные сети, системы нечеткой логики и основанные на правилах экспертные системы.

Схемы обнаружения атак разделяют на две категории:

1) обнаружение злоупотреблений; 2) обнаружение аномалий.

К первым относят атаки, которые используют известные уязвимости информационной системы, а ко вторым - несвойственную пользователям ИС деятельность.

Для обнаружения аномалий выявляется деятельность, которая отличается от шаблонов, установленных для пользователей или групп пользователей. Обнаружение аномалий, как правило, связано с созданием базы знаний, которая содержит профили контролируемой деятельности, а обнаружение злоупотреблений – со сравнением деятельности пользователя с известными шаблонами поведения хакера и использует методы на основе правил, описывающих сценарии атак. Механизм обнаружения идентифицирует потенциальные атаки в случае, если действия пользователя не совпадают с установленными правилами.

В работе [6] подчеркнуто, что проблема обеспечения защиты информации в интеллектуальных системах обработки информации является одной из важнейших при построении надежной информационной структуры. Эта проблема охватывает физическую защиту данных и системных программ и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях. Несанкционированный доступ может быть результатом деятельности как посторонних лиц, так и специальных программ-вирусов. Не менее важной задачей является оценка качества защиты информации. В данной статье предложена система оценки качества защиты информации интеллектуальных систем с учетом динамики изменения их параметров.

В работе [7] продолжено исследование основных направлений информационной безопасности интеллектуальных систем с позиции информационно-эволюционного подхода. Основное внимание в работе сконцентрировано на направлении их защиты «от информации». Статья продолжает цикл работ посвященных семантико-прагматическим аспектам обеспечения информационной безопасности.

В работе [8] с позиций общей информациологии рассматриваются прагматические аспекты обеспечения информационной безопасности в сетевых интеллектуальных системах. Формулируется проблема защиты интеллектуальных систем (естественного и искусственного, антропогенного, происхождения) «от информации» (избыточной, бесполезной или вредной, в частности ложной и иллюзорной), представляющей непосредственную либо косвенную угрозу их стабильному функционированию и развитию. Предлагаются концепция и методология разрешения поставленной проблемы, базирующаяся на совокупности методов и моделей аксиологической фильтрации семантической информации. В основу концепции защиты положена идея выявления ценной в семантическом плане (отсеивания или фильтрации бесполезной или вредной) информации, поступающей в интеллектуальную систему.

В работе [9] отмечено, что в построении интеллектуальных СЗИ достигнут в области обнаружения неизвестных СПТВ. Разработаны несколько подходов к решению проблемы достаточно достоверного их обнаружения:

- на основе нейронных сетей;
- на основе методов математической статистики;
- на основе векторных машин
- на основе генетических алгоритмов.

В работе [10] сформулированы основные требования, которым должна удовлетворять перспективная интеллектуальная ситема защиты информации:

- способность обнаруживать априорно неизвестные СПТВ;
- автоматизированная поддержка принятия решения о противодействии СПТВ;
- способность автоматического оценивания изменения уровня защищенности АС от СПТВ при изменении условий функционирования;
- автоматизированная поддержка принятия решения о перераспределении ресурсов СЗИ АС;
- автоматическое изменение своих свойств и параметров в зависимости от изменения условий среды функционирования, на основе накопления и использования информации о ней;
- способность к дезинформации нападающей стороны об истинных свойствах и параметрах АС;
- способность к снижению нецелевой нагрузки на комплекс средств автоматизации АС;
- автоматическое воздействие на ресурсы нападающей стороны (время, вычислительные и коммуникационные ресурсы).

Исходя из вышеизложенного, архитектура перспективной интеллектуальной

СЗИ АС должна включать следующие функциональные компоненты:

- подсистему обнаружения СПТВ;
- подсистему накопления данных;
- подсистему анализа защищенности;
- подсистему адаптации СЗИ;
- подсистему активного противодействия СПТВ.

В работе [11] отмечено, что при создании интеллектуальных систем противодействия таким угрозам информационной безопасности, как сетевые вторжения, вирусы и спам, необходимо анализировать интенсивный поток данных на наличие одновременно нескольких тысяч эталонных последовательностей символов. Для достижения требуемой производительности часто используют аппаратные решения на базе программируемых интегральных схем. В работе исследован зарубежный опыт подобных разработок, предложено применение унифицированных изделий.

В работе [12] рассматривается модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город» с позиции теории множеств, учитывая внутрисегментные и межсегментные вторжения злоумышленников.

В работе [13] представлена методика оценки эффективности адаптивной интеллектуальной системы защиты информации, модель которой основана на свойствах нечетких и нейронных сетей и имеет иерархическое построение по уровням и механизмам защиты.

В работе [14] представлен алгоритм функционирования модели адаптивной интеллектуальной инфокоммуникационной системы защиты информации КАИС «Безопасный город».

В работе [15] отмечено, что кибернетическое противоборство знаменует собой новый уровень информационного противоборства, имеющего место в компьютерной инфраструктуре. Новым и достаточно перспективным направлением в защите информации в условиях киберпротивоборства является построение системы интеллектуальных сервисов защиты информации. Система интеллектуальных сервисов защиты информации использует технологию управления информацией и событиями безопасности, что позволяет ей успешно противостоять кибератакам и кибертерроризму и обеспечивать необходимый уровень кибербезопасности защищаемой инфраструктуры. Рассматриваются основные положения

по построению системы интеллектуальных сервисов защиты и ее отдельных компонентов. На основании результатов рассмотрения общих положений по построению системы интеллектуальных сервисов защиты информации представлены подходы к реализации ряда базовых интеллектуальных сервисов защиты, таких как сервисы сбора, преобразования и хранения информации о событиях безопасности, сервисы моделирования атак и поведения защищаемой системы, сервисы поддержки принятия решений в области обеспечения безопасности и сервисы визуализации информации о безопасности.

В работе [16] приводится описание общей архитектуры системы интеллектуальных сервисов защиты информации (СИСЗИ), предназначенной для использования в критически важных инфраструктурах, а также входящих в ее состав компонентов. В общей архитектуре СИСЗИ выделяются три уровня: данных, событий и прикладной. Рассматриваются структурная и функциональная модели общей архитектуры СИСЗИ, позволяющие определить основные функциональные механизмы для выделенных уровней. В качестве основных компонентов СИСЗИ, для которых приводится более детальное описание их архитектурного построения, рассматриваются модуль управления корреляцией событий, прогностический анализатор безопасности, компонент моделирования атак и поведения системы защиты, компонент поддержки решений и реагирования, модуль визуализации и репозиторий.

В работе [17] приводится описание архитектуры СИСЗИ, предлагаемой для использования в критических инфраструктурах. Рассматриваются структурная и функциональная модели СИСЗИ. На их основе выделяются и рассматриваются как основные функциональные механизмы СИСЗИ механизмы обработки данных, управления моделями, поддержки решений и реагирования, визуализации и хранения данных о событиях безопасности.

В работе [18] проведен анализ открытых литературных источников, связанных с обеспечением защиты информации, циркулирующей в системах электронного документооборота (СЭД). Приведена структуризация проблемы интеллектуальной защиты информации в соответствии с нормативными документами, связанными с информационной безопасностью (ИБ) автоматизированных систем (АС). Концептуально показан перспективный путь развития систем защиты информации от НСД СЭД. Осуществлена постановка проблемы интеллектуальной защиты информации от НСД СЭД.

В работе [19] разработана концепция интеллектуальной защиты информации от НСД в СЭД, включающая систему понятий в области интеллектуальной защиты информации от НСД, гипотезы о поведении противоборствующих сторон в условиях информационного конфликта, концептуальные модели реализации воздействий злоумышленника и интеллектуальной защиты информации от НСД позволяющие определить общую методологию решения научной проблемы повышения защищенности СЭД от угроз НСД.

В работе [20] подчеркивается, что процесс защиты информации в АСК порождает целый ряд сложных проблем, решением которых является повышение защищенности автоматизированных систем критического применения (АСК) и в конечном итоге надёжности их функционирования. Для обеспечения защищенности АСК предложена принципиально новая научно-методологическая база, содержащая аргументированные ответы на вопросы, возникающие при решении проблемы разработки и эффективного управления системой интеллектуальной защиты информации (СИЗИ) АСК.

В работе [21] производится анализ уязвимостей систем интеллектуальной защиты информации. Предложенные показатели уязвимости состояний функционирования СИЗИ с точки зрения их вероятностно-временных характеристик удобны для практического применения, та как они универсальны, просты в использовании и позволяют решать задачу, в принятых предположениях, аналитически точно при малых объемах вычислений.

В работе [22] рассматривается метод комплексной оценки эффективности функционирования систем интеллектуальной защиты информации от несанкционированного доступа, включающей математические модели критериев оценки их качества.

В работе [23] обосновано, что для обнаружения атак внедрения враждебного кода и предупреждения атак других групп в состав СИЗИ должны быть включены средства идентификации безопасности форматов данных, обеспечивающие реализацию дополнительных функций.

В работе [24] в состав СИЗИ, кроме стандартных сервисных функций, включены перспективные функции по ЗИ от НСД, реализуемые с помощью подсистемы многоуровневого управления доступом пользователей к информации в АСК. Алгоритм процедуры многоуровневого управления доступом пользователей к информационным ресурсам АСК разработан в соответствии с уровнями конфиденциальности обрабатываемой информации.

В работе [25] проведен анализ публикаций о применении интеллектуальных средств для решения задач защиты информации, в частности, посвященных системам обнаружения компьютерных атак (СОА). Показано, что основным механизмом обнаружения компьютерных атак является интеллектуальный анализ данных, а основными средствами для реализации интеллектуального анализа данных – экспертные системы, нейронные сети, системы нечеткой логики и гибридные нейро-нечеткие и нейро-экспертные системы.

В работе [26] приводятся результаты разработки алгоритмического и программного обеспечения для автоматизированной поддержки принятия решений в интеллектуальной системе защиты информации, в которой при использовании экспертной информации осуществляется процесс выбора способов обеспечения требуемого уровня защищенности в течение всего периода эксплуатации объекта информатизации и при изменении условий среды функционирования.

В работе [27] анализируются основные аспекты управления защитой информации в критически важных сегментах информационных систем. Предложены модели системы управления, систем поддержки принятия решений по оперативному и организационно-техническому управлению защитой информации. Приведено формализованное описание методов принятия решений, описаны алгоритмы, реализованные в программных модулях.

В работе [28] отмечено, что на рынке инструментальных средств создания нейросетевых интеллектуальных систем представлено большое количество программных средств, что объясняется многоплановостью задач интеллектуальной обработки информации. В работе предлагается обзор инструментальных средств, применимых для создания нейросетевых компонент интеллектуальных систем защиты информации.

В работе [29] показано, что одним из основных атрибутов модели адаптивной защиты информации, в основу которой положен принцип аналогии систем информационных технологий (ИТ) и биологических систем, является наличие иерархии уровней защиты информации. Рассмотрена организация адаптивной защиты, включающей иммунный (нижний) и рецепторный (верхний) иерархические уровни. Адаптивный характер уровней защиты обусловлен использованием интеллектуальных механизмов нечеткой логики, нейронных сетей (НС) и генетических алгоритмов в иерархии классификаторов, а именно, угроз по признакам атак и механизмов защиты на поле известных угроз.

В работе [30] рассмотрена реализация основных этапов технологии разработки адаптивной системы защиты информации (СЗИ) на базе интеллектуальных средств. Представлены примеры формирования и коррекции баз данных (БД) и баз знаний (БЗ) адаптивного уровня классификации в составе СЗИ.

В работе [31] проведенный анализ инструментальных средств создания нейросетевых интеллектуальных систем показал, что на рынке этих средств представлено большое количество программных средств, что объясняется многоплановостью задач интеллектуальной обработки информации. В работе предлагается обзор инструментальных средств, применимых для создания нейросетевых компонент интеллектуальных систем защиты информации.

В работе [32] отмечается, что создание перспективных систем защиты информации (СЗИ) в последнее время отождествляют с активным использованием интеллектуальных средств, таких как экспертные системы (ЭС), системы нечеткой логики (НЛ), нейронные сети (НС), генетические алгоритмы (ГА), реализующих в СЗИ эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности (ИБ) в виде доступной для анализа системы нечетких правил If-Then. В работе дан анализ интеллектуальных средств, применяемых для решения задачи классификации объектов, предложен подход к организации квазилогических нейронечетких средств классификации.

В работе [33] рассмотрены вопросы организации системы защиты информации (СЗИ), структура которой ориентирована на процессы адаптации к динамике угроз и компьютерных атак. Показано, что в двухуровневой иерархической модели адаптивной СЗИ нижний адаптивный уровень, ответственный за оперативную реакцию на динамику внешнего окружения, должен быть интеллектуальным (по аналогии с иммунными механизмами биологической системы, которые работают автоматически, практически без коррекции со стороны центральной нервной системы), а верхний адаптивный уровень (соответствует процессам обобщения и запоминания центральной нервной системы) ориентирован на использование интеллекта администратора безопасности в качестве компонента модели.

В работе [34] предложена технология разработки ИТ-систем со встроенными функциями информационной безопасности, моделей и методик построения адаптивных средств в составе системы защиты информации, учитывающих изменение множества угроз, условий эксплуатации и ориентированных на специфику процессов, свойственных средствам интеллектуального анализа данных в режимах функционирования и обучения.

Работа [35] посвящена анализу методов сокрытия информации с помощью внедрения скрываемых данных в значения непрерывных несущих параметров речи. Рассматривается проблема измерения и модификации просодических характеристик речевого сигнала. Приводится краткий обзор работ, посвященных решению задач сокрытия данных в речевом сигнале, основанных на стегокодировании частоты основного тона и длительности вокализованных сегментов речи.

В работе [36] сформулированы задачи применения интеллектуальных методов в построении систем защиты.

Нельзя оставить без внимания работу [37], в котором предложен проект стандарта «Интегрированные интеллектуальные системы безопасности и мониторинга ситуаций на объектах и территориях». Архитектура и общие технические требования к оборудованию и программным средствам. В проекте стандарта используются ссылки на публикации [38-61]. В проекте стандарта разработаны общие принципы и технические требования по построению, применению и эксплуатации интегрированных интеллектуальных систем безопасности, предназначенных для использования на территориально-распределенных объектах транспортной инфраструктуры, крупных предприятиях, стратегически важных объектах любого масштаба и в любой точке Российской Федерации. Положения предлагаемого стандарта предназначены для использования: федеральными органами исполнительной власти; органами исполнительной власти субъектов Российской Федерации и местного самоуправления; научно-исследовательскими, проектными строительными и монтажными организациями всех форм собственности, осуществляющими проектирование, строительство, монтаж и капитальный ремонт объектов.

Выводы.

Сформулированные в настоящей работе уровни (степени) интеллектуальности систем защиты информации позволяют заново с системной точки зрения взглянуть на задачу проектирования интеллектуальных систем защиты информации.

Примечания:

1. Быковский, И. А. Философские аспекты проблем создания искусственного интеллекта. Диссертация на соискание уч. ст. канд. ф. наук. 2003. Научная библиотека диссертаций и авторефератов disserCat http://www.dissercat.com/content/filosofskie-aspekty-problem-sozdaniya-iskusstvennogo-intellekta#ixzz2hjEukM4W.

2. Дубинский А.Г. К определению понятия «интеллект». Режим доступа: http://www.iai.dn.ua /public/JournalAI_2001_4/Razdel4/18_Dubinskiy.pdf.

3. Симаворян С.Ж. Исследование и разработка методов проектирования систем защиты информации в АСУ специального назначения. Диссертация на соискание уч. ст. канд. техн. наук, ЕрНИИММ, 1991.

4. Герасименко В.А., Малюк А.А. Основы защиты информации. МГИФИ(ТУ). Отпечатано в ООО «Инкомбук» в ППО «Известия» УДПРФ. 1997г.

5. Аксенов А. Н., Андронов А. В. Интеллектуальные средства защиты информации для решения задач классификации в информационных системах. Интернет ресурс: jurnal.org/articles/2010/inf1.htm, вход 20.09.2013.
6. Анцыферов С.С., Русанов К.Е., Маслова Л.В. Защита информации интеллектуальных систем. //Искусственный интеллект. 2012. № 3. С. 430-437.
7. Баранович А.Е. Семантические аспекты информационной безопасности: концентрация знаний. //Вестник Российского государственного гуманитарного университета. 2011. № 13. С. 38-58.
8. Баранович А.Е. Прагматические аспекты информационной безопасности интеллектуальных систем. //Вестник Российского государственного гуманитарного университета. 2009. № 10. С. 56-70
9. Бородакий Ю.В., Куликов Г.В. Интеллектуальные системы обеспечения информационной безопасности. //Информационное противодействие угрозам терроризма. 2005. № 4. С. 110-112.
10. Бородакий Ю.В. Интеллектуальные системы обеспечения информационной безопасности. //Известия Южного федерального университета. Технические науки. 2005. Т. 48. № 4. С. 65-69.
11. Гильгурт С.Я. Аппаратное распознавание строк в интеллектуальных системах защиты информации.// Искусственный интеллект. 2012. № 1. С. 259-266.
12. Дунин В.С., Хохлов Н.С. Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «безопасный город». //Вестник Воронежского института МВД России. 2011. № 4. С. 74-79.
13. Дунин В.С., Бокова О.И. Оценка эффективности системы интеллектуального управления защитой информации в инфокоммуникационных системах ОВД. //Вестник Воронежского института МВД России. 2011. № 4. С. 62-73.
14. Дунин В.с., Бокова О.И., Хохлов Н.С. Алгоритм функционирования модели адаптивной системы защиты информации комплексной автоматизированной интеллектуальной системы «безопасный город». //Вестник Воронежского института МВД России. 2012. № 1. с. 151-159.
15. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства. //Труды СПИИРАН. 2012. № 3. С. 84-100.
16. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах. //Труды СПИИРАН. 2013. № 1. С. 21-40.
17. Котенко И.В., Саенко И.Б. Система интеллектуальных сервисов защиты информации для критических инфраструктур. //Технические науки - от теории к практике. 2013. № 17-1. С. 7-11.
18. Ланкин О.В. Анализ проблемы интеллектуальной защиты информации от несанкционированного доступа в системах электронного документооборота. //Вестник Воронежского государственного технического университета. 2011. Т. 7. № 4. С. 201-202.
19. Ланкин О.В. Концепция интеллектуальной защиты информации от НСД в системах электронного документооборота.// Вестник Воронежского государственного технического университета. 2011. Т. 7. № 5. С. 65-67.
20. Ланкин О.В., Сумин В.И., Воронова Е.В. Системно-комплексный кибернетический подход к формированию методологических основ интеллектуальной защиты информации от несанкционированного доступа. //Вестник Воронежского государственного технического университета. 2011. Т. 7. № 8. С. 174-176.
21. Ланкин О.В. Определение уязвимостей систем интеллектуальной защиты информации от НСД в условиях информационного противоборства. //Информация и безопасность. 2011. Т. 14. № 1. С. 97-100.
22. Ланкин О.В. Метод оценки эффективности функционирования систем интеллектуальной защиты информации от несанкционированного доступа. //Информация и безопасность. 2011. Т. 14. № 2. С. 267-270.
23. Ланкин О.В., Сумин В.И., Воронова Е.В. Метод контроля содержимого данных на наличие потенциально опасного кода в системах интеллектуальной защиты информации от несанкционированного доступа. //Вестник Воронежского государственного технического университета. 2011. Т. 7. № 9. С. 41-44.
24. Ланкин О.В., Сумин В.И., Воронова Е.В. Алгоритм процесса интеллектуальной защиты информации на основе применения дополнительных функций в системах защиты информации от НСД. //Вестник Воронежского государственного технического университета. 2011. Т. 7. № 9. С. 65-68.
25. Марченко А.А., Матвиенко С.В., Нестерук Ф.Г. К обнаружению атак в компьютерных системах нейросетевыми средствами. //Научно-технический вестник информационных технологий, механики и оптики. 2007. № 39. С. 83-93.
26. Машкина И.В., Васильев В.И. Подход к разработке интеллектуальной системы защиты информации. //Информационные технологии. 2007. № 6. С. 2-6.

27. Машкина И.В., Гузаиров М.Б. Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем. //Информационные технологии. 2008. № S7. С. 1-32.

28. Нестерук Ф.Г., Котенко И.В. Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации. //Труды СПИИРАН. 2013. № 3. С. 7-25.

29. Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Костин А.А., Воскресенский С.И. Организация иерархической защиты информации на основе интеллектуальных средств нейронечеткой классификации. //Вопросы защиты информации. 2005. № 3. С. 16-26.

30. Нестерук Ф.Г., Нестерук Л.Г. Разработка адаптивного уровня в составе системы защиты информации на базе интеллектуальных средств. //Вопросы защиты информации. 2009. № 2. С. 52-56.

31. Нестерук Ф.Г., Котенко И.В. Инструментальные средства создания нейросетевых компонент интеллектуальных систем защиты информации. //Труды СПИИРАН. 2013. № 3. С. 7-25.

32. Нестерук Ф.Г., Молдовян А.А., Нестерук Г.Ф., Нестерук Л.Г. Квазилогические нейронечеткие сети для решения задачи классификации в системах защиты информации. //Вопросы защиты информации. 2007. № 1. С. 23-31.

33. Нестерук Ф. Г. К организации интеллектуальной защиты информации. //Труды СПИРАН. 2009. № 10. С. 148 – 159.

34. Нестерук Ф.Г. К разработке технологии создания адаптивных систем защиты информации на базе интеллектуальных средств. //Вопросы защиты информации. 2009. № 1. С. 50-56.

35. Пономарь М.О. Использование вариативности речевой просодии при создании интеллектуальных систем защиты информации. //Вестник Московского государственного лингвистического университета. 2010. № 592. С. 172-175.

36. Трегубов А.Г.Построение интеллектуальных комплексов защиты информации в автоматизированных системах. //Проблемы информационной безопасности. Компьютерные системы. 2007. № 1. С. 7-10.

37. Проект стандарта «Интегрированные интеллектуальные системы безопасности и мониторинга ситуаций на объектах и территориях». Архитектура и общие технические требования к оборудованию и программным средствам. Режим доступа: http://www.integra-s.com/tk22/gost/.

38. Федеральный закон Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

39. Федеральный закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности».

40. Федеральный закон Российской Федерации от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».

41. Федеральный закон Российской Федерации от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности».

42. Перечень объектов, подлежащих государственной охране (В ред. Постановлений Правительства РФ от 22.09.1993 г., № 951 и от 30.04.2008 г., № 320). ПР-1649 от 28 сентября 2006 г. Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов. - М.: Администрация Президента РФ - С. 9.

43. СНиП 2.01.02-85 Противопожарные нормы.

44. СНиП 3.05.06-85 Электротехнические устройства.

45. СНиП 3.05.07-85 Системы автоматизации.

46. СНиП 11-01-95 Инструкция о порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений.

47. ГОСТ Р 6.30-2003 Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документации.

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

49. ГОСТ Р 22.1.12-2005 Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования.

50. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

51. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

52. ГОСТ 34.603 - 92 Информационная технология. Виды испытаний автоматизированных систем.

53. ГОСТ Р 51241-98 Системы и устройства контроля и управления доступом. Классификация. Общие технические требования и методы испытаний.

54. ГОСТ Р 51275-2006 Защита информации. Объекты информации. Факторы, воздействующие на информацию. Общие положения.

55. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

56. ГОСТ Р 51317.6.2-2007 (МЭК 61000-6-2:2005) Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых в промышленных зонах. Требования и методы испытаний.
57. ГОСТ Р 51558-2008 Средства и системы охранные телевизионные. Классификация. Общие технические требования и методы испытаний.
58. ГОСТ Р 51901.1-2002 Управление надежностью. Анализ риска технологических систем.
59. ГОСТ Р 52435-2005 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.
60. ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения.
61. ГОСТ Р ИСО 9001-2008 Системы менеджмента качества. Требования.

References:

1. Bykovskii, I. A. Filosofskie aspekty problem sozdaniya iskusstvennogo intellekta. Dissertatsiya na soiskanie uch. st. kand. f. nauk. 2003. Nauchnaya biblioteka dissertatsii i avtoreferatov disserCat http://www.dissercat.com/content/filosofskie-aspekty-problem-sozdaniya-iskusstvennogo-intellekta#ixzz2hjEukM4W.
2. Dubinskii A.G. K opredeleniyu ponyatiya «intellekt». Rezhim dostupa:http://www.iai.dn.ua/public/JournalAI_2001_4/Razdel4/18_Dubinskiy.pdf.
3. Simavoryan S.Zh. Issledovanie i razrabotka metodov proektirovaniya sistem zashchity informatsii v ASU spetsial'nogo naznacheniya. Dissertatsiya na soiskanie uch. st. kand. tekhn. nauk, ErNIIMM, 1991.
4. Gerasimenko V.A., Malyuk A.A. Osnovy zashchity informatsii. MGIFI(TU). Otpechatano v OOO «Inkombuk» v PPO «Izvestiya» UDPRF. 1997g.
5. Aksenov A. N., Andronov A. V. Intellektual'nye sredstva zashchity informatsii dlya resheniya zadach klassi¬fikatsii v informatsionnykh sistemakh. Internet resurs: jurnal.org/articles/2010/inf1.htm, vkhod 20.09.2013.
6. Antsyferov S.S., Rusanov K.E., Maslova L.V. Zashchita informatsii intellektual'nykh sistem. //Iskusstvennyi intellekt. 2012. № 3. S. 430-437.
7. Baranovich A.E. Semanticheskie aspekty informatsionnoi bezopasnosti: kontsentratsiya znanii. //Vestnik Rossiiskogo gosudarstvennogo gumanitarnogo universiteta. 2011. № 13. S. 38-58.
8. Baranovich A.E. Pragmaticheskie aspekty informatsionnoi bezopasnosti intellektual'nykh sistem. //Vestnik Rossiiskogo gosudarstvennogo gumanitarnogo universiteta. 2009. № 10. S. 56-70
9. Borodakii Yu.V., Kulikov G.V. Intellektual'nye sistemy obespecheniya informatsionnoi bezopasnosti. //Informatsionnoe protivodeistvie ugrozam terrorizma. 2005. № 4. S. 110-112.
10. Borodakii Yu.V. Intellektual'nye sistemy obespecheniya informatsionnoi bezopasnosti. //Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. 2005. T. 48. № 4. S. 65-69.
11. Gil'gurt S.Ya. Apparatnoe raspoznavanie strok v intellektual'nykh sistemakh zashchity informatsii.// Iskusstvennyi intellekt. 2012. № 1. S. 259-266.
12. Dunin V.S., Khokhlov N.S. Model' ugroz informatsionnoi bezopasnosti kompleksnoi avtomatizirovannoi intellektual'noi sistemy «bezopasnyi gorod». //Vestnik Voronezhskogo instituta MVD Rossii. 2011. № 4. S. 74-79.
13. Dunin V.S., Bokova O.I. Otsenka effektivnosti sistemy intellektual'nogo upravleniya zashchitoi informatsii v infokommunikatsionnykh sistemakh OVD. //Vestnik Voronezhskogo instituta MVD Rossii. 2011. № 4. S. 62-73.
14. Dunin V.s., Bokova O.I., Khokhlov N.S. Algoritm funktsionirovaniya modeli adaptivnoi sistemy zashchity informatsii kompleksnoi avtomatizirovannoi intellektual'noi sistemy «bezopasnyi gorod». //Vestnik Voronezhskogo instituta MVD Rossii. 2012. № 1. s. 151-159.
15. Kotenko I.V., Saenko I.B. Postroenie sistemy intellektual'nykh servisov dlya zashchity informatsii v usloviyakh kiberneticheskogo protivoborstva. //Trudy SPIIRAN. 2012. № 3. S. 84-100.
16. Kotenko I.V., Saenko I.B. Arkhitektura sistemy intellektual'nykh servisov zashchity informatsii v kriticheski vazhnykh infrastrukturakh. //Trudy SPIIRAN. 2013. № 1. S. 21-40.
17. Kotenko I.V., Saenko I.B. Sistema intellektual'nykh servisov zashchity informatsii dlya kriticheskikh infrastruktur. //Tekhnicheskie nauki - ot teorii k praktike. 2013. № 17-1. S. 7-11.
18. Lankin O.V. Analiz problemy intellektual'noi zashchity informatsii ot nesanktsionirovannogo dostupa v sistemakh elektronnogo dokumentooborota. //Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. T. 7. № 4. S. 201-202.
19. Lankin O.V. Kontseptsiya intellektual'noi zashchity informatsii ot NSD v sistemakh elektronnogo dokumentooborota.// Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. T. 7. № 5. S. 65-67.

20. Lankin O.V., Sumin V.I., Voronova E.V. Sistemno-kompleksnyi kiberneticheskii podkhod k formirovaniyu metodologicheskikh osnov intellektual'noi zashchity informatsii ot nesanktsionirovannogo dostupa. //Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. T. 7. № 8. S. 174-176.
21. Lankin O.V. Opredelenie uyazvimostei sistem intellektual'noi zashchity informatsii ot NSD v usloviyakh informatsionnogo protivoborstva. //Informatsiya i bezopasnost'. 2011. T. 14. № 1. S. 97-100.
22. Lankin O.V. Metod otsenki effektivnosti funktsionirovaniya sistem intellektual'noi zashchity informatsii ot nesanktsionirovannogo dostupa. //Informatsiya i bezopasnost'. 2011. T. 14. № 2. S. 267-270.
23. Lankin O.V., Sumin V.I., Voronova E.V. Metod kontrolya soderzhimogo dannykh na nalichie potentsial'no opasnogo koda v sistemakh intellektual'noi zashchity informatsii ot nesanktsionirovannogo dostupa. //Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. T. 7. № 9. S. 41-44.
24. Lankin O.V., Sumin V.I., Voronova E.V. Algoritm protsessa intellektual'noi zashchity informatsii na osnove primeneniya dopolnitel'nykh funktsii v sistemakh zashchity informatsii ot NSD. //Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. T. 7. № 9. S. 65-68.
25. Marchenko A.A., Matvienko S.V., Nesteruk F.G. K obnaruzheniyu atak v komp'yuternykh sistemakh neirosetevymi sredstvami. //Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki. 2007. № 39. S. 83-93.
26. Mashkina I.V., Vasil'ev V.I. Podkhod k razrabotke intellektual'noi sistemy zashchity informatsii. //Informatsionnye tekhnologii. 2007. № 6. S. 2-6.
27. Mashkina I.V., Guzairov M.B. Intellektual'naya podderzhka prinyatiya reshenii po upravleniyu zashchitoi informatsii v kriticheski vazhnykh segmentakh informatsionnykh sistem. //Informatsionnye tekhnologii. 2008. № S7. S. 1-32.
28. Nesteruk F.G., Kotenko I.V. Instrumental'nye sredstva sozdaniya neirosetevykh komponent intellektual'nykh sistem zashchity informatsii. //Trudy SPIIRAN. 2013. № 3. S. 7-25.
29. Nesteruk G.F., Moldovyan A.A., Nesteruk F.G., Kostin A.A., Voskresenskii S.I. Organizatsiya ierarkhicheskoi zashchity informatsii na osnove intellektual'nykh sredstv neironechetkoi klassifikatsii. //Voprosy zashchity informatsii. 2005. № 3. S. 16-26.
30. Nesteruk F.G., Nesteruk L.G. Razrabotka adaptivnogo urovnya v sostave sistemy zashchity informatsii na baze intellektual'nykh sredstv. //Voprosy zashchity informatsii. 2009. № 2. S. 52-56.
31. Nesteruk F.G., Kotenko I.V. Instrumental'nye sredstva sozdaniya neirosetevykh komponent intellektual'nykh sistem zashchity informatsii. //Trudy SPIIRAN. 2013. № 3. S. 7-25.
32. Nesteruk F.G., Moldovyan A.A., Nesteruk G.F., Nesteruk L.G. Kvazilogicheskie neironechetkie seti dlya resheniya zadachi klassifikatsii v sistemakh zashchity informatsii. //Voprosy zashchity informatsii. 2007. № 1. S. 23-31.
33. Nesteruk F. G. K organizatsii intellektual'noi zashchity informatsii. //Trudy SPIRAN. 2009. № 10. S. 148 – 159.
34. Nesteruk F.G. K razrabotke tekhnologii sozdaniya adaptivnykh sistem zashchity informatsii na baze intellektual'nykh sredstv. //Voprosy zashchity informatsii. 2009. № 1. S. 50-56.
35. Ponomar' M.O. Ispol'zovanie variativnosti rechevoi prosodii pri sozdanii intellektual'nykh sistem zashchity informatsii. //Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. 2010. № 592. S. 172-175.
36. Tregubov A.G.Postroenie intellektual'nykh kompleksov zashchity informatsii v avtomatizirovannykh sistemakh. //Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy. 2007. № 1. S. 7-10.
37. Proekt standarta «Integrirovannye intellektual'nye sistemy bezopasnosti i monitoringa situatsii na ob"ektakh i territoriyakh». Arkhitektura i obshchie tekhnicheskie trebovaniya k oborudovaniyu i programmnym sredstvam. Rezhim dostupa: http://www.integra-s.com/tk22/gost/.
38. Federal'nyi zakon Rossiiskoi Federatsii ot 27 dekabrya 2002 g. № 184-FZ «O tekhnicheskom regulirovanii».
39. Federal'nyi zakon Rossiiskoi Federatsii ot 5 marta 1992 g. № 2446-1 «O bezopasnosti».
40. Federal'nyi zakon Rossiiskoi Federatsii ot 21 dekabrya 1994 g. № 68-FZ «O zashchite naseleniya i territorii ot chrezvychainykh situatsii prirodnogo i tekhnogennogo kharaktera».
41. Federal'nyi zakon Rossiiskoi Federatsii ot 22 iyulya 2008 g. № 123-FZ «Tekhnicheskii reglament o trebovaniyakh pozharnoi bezopasnosti».
42. Perechen' ob"ektov, podlezhashchikh gosudarstvennoi okhrane (V red. Postanovlenii Pravitel'stva RF ot 22.09.1993 g., № 951 i ot 30.04.2008 g., № 320). PR-1649 ot 28 sentyabrya 2006 g. Osnovy gosudarstvennoi politiki v oblasti obespecheniya bezopasnosti naseleniya Rossiiskoi Federatsii i zashchishchennosti kriticheski vazhnykh i potentsial'no opasnykh ob"ektov ot ugroz tekhnogennogo, prirodnogo kharaktera i terroristicheskikh aktov. - M.: Administratsiya Prezidenta RF - S. 9.
43. SNiP 2.01.02-85 Protivopozharnye normy.
44. SNiP 3.05.06-85 Elektrotekhnicheskie ustroistva.
45. SNiP 3.05.07-85 Sistemy avtomatizatsii.

46. SNiP 11-01-95 Instruktsiya o poryadke razrabotki, soglasovaniya, utverzhdeniya i sostave proektnoi dokumentatsii na stroitel'stvo predpriyatii, zdanii i sooruzhenii.
47. GOST R 6.30-2003 Unifitsirovannye sistemy dokumentatsii. Unifitsirovannaya sistema organizatsionno-rasporyaditel'noi dokumentatsii. Trebovaniya k oformleniyu dokumentatsii.
48. GOST R 53704-2009 Sistemy bezopasnosti kompleksnye i integrirovannye. Obshchie tekhnicheskie trebovaniya.
49. GOST R 22.1.12-2005 Strukturirovannaya sistema monitoringa i upravleniya inzhenernymi sistemami zdanii i sooruzhenii. Obshchie trebovaniya.
50. GOST 34.003-90 Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Avtomatizirovannye sistemy. Terminy i opredeleniya.
51. GOST 34.601-90 Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Avtomatizirovannye sistemy. Stadii sozdaniya.
52. GOST 34.603 - 92 Informatsionnaya tekhnologiya. Vidy ispytanii avtomatizirovannykh sistem.
53. GOST R 51241-98 Sistemy i ustroistva kontrolya i upravleniya dostupom. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya i metody ispytanii.
54. GOST R 51275-2006 Zashchita informatsii. Ob"ekty informatsii. Faktory, vozdeistvuyushchie na informatsiyu. Obshchie polozheniya.
55. GOST R 50922-2006 Zashchita informatsii. Osnovnye terminy i opredeleniya.
56. GOST R 51317.6.2-2007 (MEK 61000-6-2:2005) Sovmestimost' tekhnicheskikh sredstv elektromagnitnaya. Ustoichivost' k elektromagnitnym pomekham tekhnicheskikh sredstv, primenyaemykh v promyshlennykh zonakh. Trebovaniya i metody ispytanii.
57. GOST R 51558-2008 Sredstva i sistemy okhrannye televizionnye. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya i metody ispytanii.
58. GOST R 51901.1-2002 Upravlenie nadezhnost'yu. Analiz riska tekhnologicheskikh sistem.
59. GOST R 52435-2005 Tekhnicheskie sredstva okhrannoi signalizatsii. Klassifikatsiya. Obshchie tekhnicheskie trebovaniya i metody ispytanii.
60. GOST R 52551-2006 Sistemy okhrany i bezopasnosti. Terminy i opredeleniya.
61. GOST R ISO 9001-2008 Sistemy menedzhmenta kachestva. Trebovaniya.

УДК 004.89

Об одном подходе к вопросу о классификации интеллектуальных систем защиты информации

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

[1-3] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
[1] кандидат технических наук, доцент
E-mail: simsim58@mail.ru
[2] кандидат физ.-мат. наук, доцент
E-mail: oppm@mail.ru
[3]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 производится анализ литературы по вопросу определения интеллектуальности систем защиты информации. В результате анализа сделан вывод о расширении понятия интеллектуальности систем защиты информации. Дана новая классификация, которая значительно шире даёт взгляд на эту проблему.

Ключевые слова: интеллектуальные системы защиты информации, уровни интеллектуальности.