ISSN 2306-1561
Automation and Control in Technical Systems (ACTS)
2014, No 1.1(8), pp. 55-61.
DOI: 10.12731/2306-1561-2014-1-6

Review of the technology, tools and policies to ensure information security and computer intelligent systems

Sirajova Zulayho Giyaziddinovna

Uzbekistan Republic, Undergraduate Student, Department of «Automated Control Systems».

Moscow Automobile & Road construction State Technical University, 125319, Russian Federation, Moscow, Leningradsky prospekt, 64. Tel.: +7 (499) 151-64-12. http://www.madi.ru

schastye7@bk.ru

Abstract. The article is a brief study of existing theoretical and methodological approaches to provision of the computer and information security of intelligent systems. The computer and information security of intelligent systems is a sophisticated integrated object which requires special management approaches. The article contains key provisions of the security policy for intelligent systems and considers key types of threats for the information and computer security of intelligent systems. The policy for the computer and information security is not only a reasonably required document regulating the use of intelligent systems for fulfillment of user's duties. The policy for computer and information security is a set of efficient practical measures aimed at prevention and avoidance of threats to stability and nonsusceptibility of the system's performance.

Keywords: intelligent systems, artificial intelligence, tools and systems for the protection of information security threat, the threat of information leakage, the object information, vulnerability, information security policy, information security, computer security.

ISSN 2306-1561
Автоматизация и управление в технических системах (АУТС)
2014. – №1.1(8). – С. 55-61.
DOI: 10.12731/2306-1561-2014-1-6

УДК 004.8

Обзор технологии, средств обеспечения и политики компьютерной и информационной безопасности интеллектуальных систем

Сиражова Зулайхо Гиязиддиновна

Республика Узбекистан, магистрант кафедры «Автоматизированные системы управления».

ФГБОУ ВПО «Московский автомобильно-дорожный государственный технический университет (МАДИ)», 125319, Российская Федерация, г. Москва, Ленинградский проспект, д.64, Тел.: +7 (499) 151-64-12, http://www.madi.ru

schastye7@bk.ru

Аннотация. Статья представляет собой краткое исследование существующих на сегодняшний день теоретических и методологических подходов к обеспечению компьютерной и информационной безопасности интеллектуальных систем. В работе показано, что информационная и компьютерная безопасность интеллектуальных систем представляет собой сложный интегрированный объект, который требует особых управленческих подходов. Также в статье раскрываются основные положения политики безопасности в интеллектуальных системах и рассматриваются основные типы угроз информационной и компьютерной безопасности интеллектуальных систем. Политика информационно-компьютерной безопасности это не только объективно необходимый документ, регламентирующий использование интеллектуальных систем для выполнения каких-либо должностных обязанностей пользователей. Но и также политика информационно-компьютерной безопасности представляет собой совокупность действенных практических мер, направленных на предупреждение и недопущение реализации угроз в отношении стабильности и неуязвимости функционирования самой системы.

Ключевые слова: интеллектуальные системы, системы искусственного интеллекта, средства и системы защиты, угроза безопасности информации, угроза утечки информации, объект информатизации, уязвимость системы, политика информационной безопасности, информационная безопасность, компьютерная безопасность.

1. Введение

Изменения, происходящие в современных системах и структурах (властных управленческих органах, предприятиях, общественных организациях и т.д.), использующих для реализации своих функций различные интеллектуальные системы настолько быстротечны, а перечень хранимой и необходимой для деятельности информации настолько велик и в достаточной степени конфиденциален, что весьма часто именно используемые в работе интеллектуальные системы становятся объектом сторонних неправомерных действий. Эти сторонние действия имеют своей целью получить доступ к данным и информации, которые хранит, анализирует и обрабатывает интеллектуальная система, последствия же таких действий объективно предсказуемы и очевидны, и выражаются они, как правило, в нанесении ущерба той структуре, которая в своём управлении использует интеллектуальные системы. При этом не стоит забывать о том, что не только сторонние неправомерные действия могут быть направлены на получение данных и информации, хранящейся в интеллектуальной системе. Весьма часто интеллектуальные системы становятся объектом вредоносного вмешательства со стороны пользователей этой системы. И эти действия могут иметь как случайный разовый характер, не имеющими своей целью нанесения тотального вреда системе, так и быть неслучайными, но планомерными, имеющими нелегитимные цели. Поэтому использование специальных технологий, средств обеспечения компьютерной и информационной безопасности интеллектуальных систем, а также формирование и регулярное обновление политики безопасности в этих системах становится особенно актуальным [1 – 15].

Цель данной работы состоит в кратком анализе основного теоретического и практического инструментария, применяемого при формировании политики безопасности интеллектуальных систем, используемых в управлении различными объектами народнохозяйственного назначения. Задачи данной работы сводятся к следующему:

- представить основные термины и определения, которые относятся к сфере обеспечения информационной и компьютерной безопасности интеллектуальных систем;
- изложить базовые основы обеспечения информационной и компьютерной безопасности интеллектуальных систем;
- раскрыть основные подходы к формированию политики безопасности в интеллектуальных системах.

2. Терминологический аппарат и теоретические основания обеспечения информационной и компьютерной безопасности интеллектуальных систем

В первую очередь необходимо определиться с понятием «интеллектуальные системы». Очевидно, что данное понятие напрямую связано с искусственным интеллектом. Интеллектуальная система представляет собой сложный программно-

технический объект, который имеет конкретное назначение – решение специального рода задач, относимых к творческим или креативным. Интеллектуальная система, таким образом, может рассматриваться как компьютерная модель умственно-интеллектуальных возможностей человека. Функционирование такой системы выражается через целенаправленный поиск, анализ и синтез информации об окружающей действительности для получения новых знаний об этой действительности и решения соответствующих задач, связанных с активностью человека (групп людей или организаций) в этой действительности [7].

Понятие «информационная безопасность» рассматривается в некотором прикладном и теоретическом множестве ракурсов. Так, например, принято говорить об информационной безопасности личности, субъектов общественного или народнохозяйственного сектора, государства и т.д. [9]. Информационная безопасность может трактоваться в функциональном и процессом аспекте. С точки зрения функционального аспекта информационная безопасность есть действия ответственных исполнителей, направленные на обеспечение сохранности информационных ресурсов (данных), защищённости законных прав индивидов, их групп или общества в информационной сфере. С точки зрения процесса информационная безопасность есть процесс обеспечения конфиденциальности, целостности и доступности информации.

В свою очередь компьютерная безопасность представляет собой такое состояние системы, в том числе и интеллектуальной, при котором эта система не неуязвима [4]. То есть компьютерная безопасность представляет собой такие меры и действия, которые направлены на предупреждение нарушения целостности интеллектуальной системы и/или на предупреждение нарушений в её функционировании. Выше сказанное позволяет нам говорить об интегрированном представлении информационно-компьютерной безопасности интеллектуальных систем.

Вместе с тем существует перечень способов, направленных на обеспечение информационно-компьютерной безопасности интеллектуальных систем. Эти способы можно определить как совокупность средств, методов и инструментов, используемых для обеспечения безопасности и противодействия уязвимости интеллектуальных систем и направленных на сохранение конфиденциальности, целостности и доступности информации, имеющейся в базах данных системы, а также направленных на сохранение целостности и функциональности самой системы.

Цели информационно-компьютерной безопасности интеллектуальных систем состоит в формировании такой совокупности мер при должном инструментальном и методическом обеспечении, позволяющим гарантировать пользователям данной интеллектуальной системы сохранность основных качеств хранимой в базе данных информации, а также неуязвимое, эффективное и качественное функционирование самой системы в процессе её эксплуатации (в рамках решения основных пользовательских задач).

Для достижения цели обеспечения информационно-компьютерной безопасности интеллектуальных систем на организационно-управленческом уровне должны быть решены следующие технологические задачи [7]:

- провести идентификацию и классификацию информационных ресурсов, а также технологий, средств и приложений, используемых для их обработки;
- провести идентификацию и классификацию всех возможных внутренних и внешних угроз информационно-компьютерной безопасности используемой интеллектуальной системы;
- провести идентификацию уязвимых мест в рамках каждой выявленной угрозы и сформулировать перечень упреждающих и контрмер, направленных на нивелирование угроз;
- оценить единичные риски и совокупный риск информационно-компьютерной опасности используемой интеллектуальной системе.

Идентификация и классификация всех возможных рисков и угроз является основой не только для формулировки контрмер противодействия и/или предупреждения информационно-компьютерной опасности для используемой интеллектуальной системы, но и для разработки комплексной и сбалансированной политики обеспечения информационно-компьютерной безопасности.

3. Сущность и содержание политики информационно-компьютерной безопасности интеллектуальных систем

Политика информационно-компьютерной безопасности для используемых интеллектуальных систем представляет собой, как правило, нормативный документ (локальный нормативный акт), который полностью и последовательно регламентирует комплекс мер, направленных на достижение указанной выше цели рассматриваемого вида безопасности, и решения соответствующих достижению этой цели задач.

Политика информационно-компьютерной безопасности интеллектуальных систем определяет основные объекты защиты, среди которых необходимо выделить [8]:

- информационные ресурсы, которые составляют коммерческую, государственную или иную тайну;
- информационные ресурсы, которые не составляют коммерческую, государственную или прочие виды тайн, но содержат сведения или данные конфиденциального характера и ограниченного пользования и распространения;
- информационная инфраструктура, в том числе программных средства, приложения, средства и способы передачи открытой и закрытой информации.

К объектам защиты стоит отнести в первую очередь разработчиков и пользователей интеллектуальных систем, которые используют в своей трудовой (управленческой, общественной, политической, научной, государственной) деятельности эти системы для исполнения своих функций (должностных и прочих обязанностей).

Кроме определения целей, задач, объектов и субъектов обеспечения информационно-компьютерной безопасности при использовании интеллектуальных систем, соответствующая политика структурирует перечень основных угроз

рассматриваемого вида безопасности и модель нарушителя этой безопасности. Как правило, все угрозы классифицируются по уровням (высокий, средний, низкий уровень угроз) и по основным группам [6]:

- угрозы антропогенного характера, т.е. угрозы, обусловленные деятельностью человека;
- угрозы техногенного характера, т.е. обусловленные функционированием аппаратных средств, машин, механизмов и электронных устройств;
- угрозы естественного характера, т.е. возникающие в результате действия природных сил.

Поскольку угрозы антропогенного характера наиболее значимы, а их вероятность возникновения в виде соответствующих рисков весьма высока, политика информационно-компьютерной безопасности интеллектуальных систем включает формализацию модели нарушителя безопасности. Все нарушителя безопасности составляют два основных класса: внутренние и внешние. Первый класс нарушителей образован сотрудниками той или иной структуры, использующей интеллектуальную систему. Во второй класс относят нарушителей, которые являются контрагентами этой структуры, а также бывшими сотрудниками, имеющими представление об алгоритмах и принципах функционирования интеллектуальной системы. Можно также выделить и объединённый класс нарушителей (например, внешний нарушитель действует в сговоре с внутренним нарушителем).

Политика информационно-компьютерной безопасности интеллектуальных систем должна включать перечень конкретных организационных, технических, физических и прочих мер по обеспечению этого вида безопасности, а также определять средства контроля над рассматриваемым видом безопасности.

4. Заключение

Обеспечение информационной и компьютерной безопасности интеллектуальных систем является интегрированной и комплексной задачей, решение которой позволяет обеспечить сохранность, конфиденциальность, целостность и доступность информационных ресурсов, хранимых в базе данных интеллектуальных систем. Интеллектуальная система представляет собой сложный объект, включающий некоторое множество программных и аппаратных средств, обеспечивающих в том числе эффективное ведение деятельности какой-либо структуры (предприятия, органа власти, общественной или научной организации). Уровень уязвимости интеллектуальных систем может быть достаточно высоким, сформированным множеством факторов внешней и внутренней среды. Для регламентации действий и мер, направленных на обеспечение информационно-компьютерной безопасности интеллектуальных систем разрабатывается специальная политика. Эта политика представляет собой программный и последовательный документ, в котором определены меры противодействия и предупреждения угроз информационно-компьютерной безопасности интеллектуальных систем, а также изложены контрольные меры и используемые для этого инструменты.

Список информационных источников

[1] Антонов П.Д. User Is A Great Obstacle For Security Systems / П.Д. Антонов, А.В. Остроух // Молодой ученый. - 2011. - №4. Т.3. - С. 62-63.

[2] Белоусова А.И. Подход к формированию многоуровневой модели мультиагентной системы с использованием миваров / А.И. Белоусова, О.О. Варламов, М.Н. Краснянский, А.В. Остроух // Перспективы науки – Тамбов. «ТМБПринт», 2011. - № 5(20). - С. 57-61.

[3] Васюгова С.А. Исследование перспектив и проблем интеграции человека с компьютером: искусственный интеллект, робототехника, технологическая сингулярность и виртуальная реальность / А.В. Остроух, С.А. Васюгова, М.Н. Краснянский, А. Самаратунга // Перспективы науки. – Тамбов: «ТМБПринт», 2011. - № 4(19). - С. 109 – 112.

[4] Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2009. – 256 с.

[5] Липовская Е.П. Методологические и технологические основы создания адаптивных интеллектуальных систем обучения сложным технологическим процессам на основе компьютерных тренажерных систем // Технико-технологические проблемы сервиса. – 2011. – №15. – С.50 – 61.

[6] Мельников В.П. Информационная безопасность и защита информации: 3 -е изд. – М.: Академия, 2010. – 338 с.

[7] Остроух А.В. Интеллектуальные системы в науке и производстве: учеб. пособие / А.В. Остроух, А.Б. Николаев. – Palmarium Academic Publishing. Saarbrucken, Germany. – 2012. - 312 с.

[8] Остроух А.В. Основы построения систем искусственного интеллекта для промышленных и строительных предприятий: монография / А.В. Остроух. – М.: ООО «Техполиграфцентр», 2008. - 280 с. - ISBN 978-5-94385-033-2.

[9] Остроух А.В. Системы искусственного интеллекта в промышленности, робототехнике и транспортном комплексе: монография / А.В. Остроух - Красноярск: Научно-инновационный центр, 2013. – 326 с. - ISBN 978-5-906314-10-9.

[10] Остроух А.В. Ввод и обработка цифровой информации: учебник для нач. проф. образования / А.В. Остроух. – М.: Издательский центр «Академия», 2012. – 288 с. - ISBN 978-5-7695-9457-1.

[11] Остроух А.В. Информационные технологии в научной и производственной деятельности / [ред. А.В. Остроух] - М: ООО "Техполиграфцентр", 2011. - 240 с. - ISBN 978-5-94385-056-1.

[12] Остроух А.В., Николаев А.Б., Сальный А.Г., Кухаренко В.Н. Общие принципы построения SCADA-систем // Автоматизация и управление в технических системах. – 2013. – № 2(4). – С. 8-12.

[13] Остроух А.В., Тянь Юань Разработка системы мониторинга производственно-технологической деятельности промышленных предприятий Китая // Автоматизация и управление в технических системах. – 2013. – № 2(4). – С. 73-76.

[14] Прангишвили И.В., Потоцкий В.А., Гинсберг К.С., Смолянинов В.В. Идентификация систем и задачи управления: на пути к современным системным методологиям // Проблемы управления. – 2010. – №4. – С.108 – 114

[15] Щеглов А.А. Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2011. – 218 с.