Эффективность расчёта параметра репутации определяется тремя обязательными правилами:

- продолжительность жизни оцениваемого объекта (в случае, если на каждый сеанс общения вырабатывается новый объект, невозможно использовать накопленные знания о нём);

- своевременность оценки текущих взаимодействий (значение параметра репутации должно корректироваться в соответствии с новым полученным знанием об объекте);

- накопление знаний об объекте (оценки предыдущих взаимодействий должны учитываться при общей оценке репутации, если они вообще были получены).

Немаловажной составляющей доверия является среда взаимодействия участников, в которой реализуются механизмы репутации и доверия. В виду того, что методики оценки доверия решают в первую очередь технические задачи, в качестве среды взаимодействия обычно рассматриваются электронные рынки, пиринговые сети, каналы передачи данных и т.д.

По своей сути, основной характеристикой среды взаимодействия является надёжность выбранного канала взаимодействия (отсутствие возможности искажения, раскрытия конфиденциальности и отказа доступа к информации). Вместе с тем, в большинстве существующих методов оценки доверия среда взаимодействия рассматривается, как контекст для выбора той или иной модели.

Однако, контекстная зависимость имеет более широкую сферу применения. Она определяет предметную область, в которой будет происходить оценка. Существуют и многоконтекстные модели, в которых каждому пользователю ставится в соответствие несколько различных моделей доверия, что значительно усложняет производимую оценку доверия. В связи с этим, большинство моделей доверия работает в одноконтекстном режиме и рассматривает ограниченные, конкретные задачи.

Анализ существующих базовых формальных подходов к оценке доверия

Среди множества существующих вычислительных моделей (метрик) оценки доверия можно выделить примитивные или базовые модели, отвечающие основным требованиям к расчёту значений доверия.

Существующие базовые системы, используют по отдельности такие механизмы, как:

- взятие среднего арифметического значения репутации, без дальнейшего расчёта доверия (eBay);

- расчёт доверия в диапазоне (-1; 1), с учётом невозможности достижения крайних значений (Marsh);

- использование понятия риска на основе таких понятий, как субъективные полезность и важность ситуации (Marsh);

- введение понятия порога доверия, когда возможность доверия зависит от некоторого минимально допустимого значения, при дополнительном введении понятия взаимности, влияющем на рассчётное значение доверия (Marsh);

- обязательное введение априори доверенных объектов - ядра доверия, влияющего на последующее формирование цепей (потоков) доверенных объектов (Advogato Trust Metric) [4].

Все указанные механизмы являются очевидно целесообразными и активно развиваются (Marsh) [4]. Однако, необходимо отметить тот факт, что использование этих механизмов может быть гораздо более объективным и точным при их использовании в совокупности. Так указанный ранее Marsh не учитывает расчёта репутации, а Advogato Trust Metric нуждается в обязательном выборе непоколебимо доверенных объектов, что продиктовано его целевым применением в социальных сетях и блогах для защиты от спама и нежелательных сообщений.

Литература

1. Полянская О.Ю. Инфраструктуры открытых ключей: учебное пособие / О.Ю. Полянская, В.С. Горбатов. – М.: Издательство «Открытые системы», 2007. – 370 с.

2. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков. - Ползуновский Вестник №2/1 2012 – С. 61-67

3. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие – М.: Издательский центр «Академия», 2009. – 272 с.

4. Marsh S. Formalising Trust as a Computational Concept. 1994. Ph.D. dissertation, University of Stirling.

И.М. Янников [1], М.В. Телегина[1], В.А. Куделькин [2]

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ОБСЛУЖИВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ И ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

([1]Ижевский государственный технический университет имени М.Т. Калашникова, г. Ижевск, [2] Консорциум «Интегра-С», г. Самара)

В настоящее время тенденции развития современных систем физической защиты (СФЗ) критически важных для национальной безопасности (КВО) и потенциально опасных объектов (ПОО) связаны с использованием новейших разработок технических средств контроля и охраны и переходом к интегрированным системам безопасности, представляющим собой сложные территориально распределённые автоматизированные системы сбора и обработки информации

о состоянии охраняемого объекта сопряжённые с необходимыми организационно-управленческими мероприятиями по охране и реагированию [1-3].

Поскольку нарушение физической безопасности объектов обычно готовится заблаговременно с упором на имеющиеся структурные и иные недостатки в системе защиты, то разработка методов оценки состояния защищенности КВО, ПОО в автоматизированном режиме крайне важна для оперативного реагирования системы защиты на нарушение режима безопасности с целью автоматического анализа ситуации и немедленного реагирования. Вышеуказанные тенденции построения современных систем физической защиты критически важных и потенциально опасных объектов учтены при разработке модели СФЗ в рамках комплексной системы безопасности КВО, ПОО (рис. 1).

Комплекс инженерно-технических средств охраны (ИТСО) определяется для каждого конкретного объекта и состоит из технических и инженерных средств охраны. Как известно, к техническим средствам физической защиты относятся [4]:

- средства охранной сигнализации служебных помещений и периметра;
- средства контроля прохода (доступа), установленные на КПП и объектах охраны;
- средства наблюдения за периметрами охраняемых зон и объектами охраны;
- средства специальной связи (в том числе — экстренной);
- средства обнаружения проноса (провоза) запрещенных средств, (в том числе носителей конфиденциальной информации);
- средства систем жизнеобеспечения (электропитания, освещения и др.).

На основе указанных общих классификационных признаков СФЗ, а также факторов, определяющих условия их применения были сформированы группы ключевых характеристик данных средств. К таковым характеристикам относятся рыночные, основные и дополнительные технические характеристики, характеристики помехоустойчивости и параметры установки, при которых обеспечиваются заданные характеристики и функциональность с наибольшей эффективностью [5].

Предлагаемая автоматизированная система контроля обслуживания технических средств охраны систем физической защиты выполняет следующие функции: формирование карт регламентных работ; мониторинг технического оборудования; контроль состояния оборудования по технической документации; контроль обслуживания серверного оборудования. Разработанная схема работы системы показывает, как обеспечивается автоматизация контроля обслуживания технических средств СФЗ объектов (рис. 2).

В системе контроля технического оборудования, по графикам проведения технического обслуживания, формируется карта регламентных работ. По результатам работы системы мониторинга оборудования, возможен внеплановый запрос на соответствующее техническое обслуживание. Контроль обслуживания серверного оборудования можно осуществить обнаружением фактов уменьшения температуры компонентов, оборотов вентиляторов, стабилизация питающих напряжений и т.д.

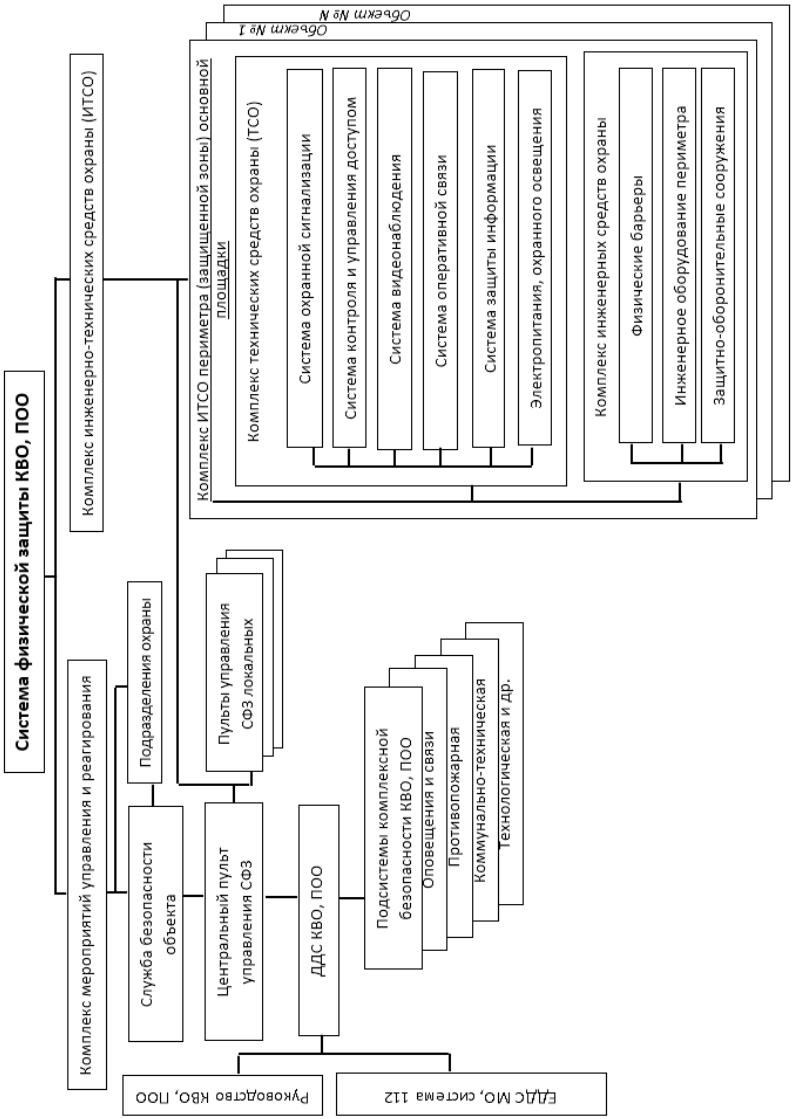

Рис. 1. Структурная модель системы физической защиты объектов

Рис. 2. Структурная схема работы программы

Для автоматизированного получения информации о необходимости технического обслуживания технических средств охраны конкретных СФЗ необходимо получить информацию о сбоях и срабатывании датчиков СФЗ, руководствоваться требованиями нормативной документации и руководства пользователя, а также соблюдать график проведения обслуживания технических средств. Информация о состоянии технических средств СФЗ попадает в базу программы, где по графику осуществляется проверка поступивших данных с

параметрами эталонных показателей. Далее формируется карта регламентных работ и рекомендации о необходимости обслуживания.

В предлагаемой программе используется архитектура клиент-сервер. Разработано три приложения: сервер, клиент и приложение, которое генерирует файлы с показаниями объектов. В качестве показаний объектов используются температура объекта, скорость вращения вентилятора на объекте и напряжение питания.

Для идентификации клиентов используется персональный идентификатор клиента, который задается на клиентской стороне. Сервер обрабатывает три запроса от клиентского приложения: подключение и отключение клиента, и результат проверки параметров. В случае, если результат проверки параметров отрицательный, сервер помещает в специальную очередь информацию об объектах, требующих ремонт. Эта информация представляет собой идентификатор объекта и его параметры до ремонта. Так же на сервере существует расписание запланированных ремонтных работ для объекта.

Полностью разработанный комплекс содержит три приложения: FileGen, SensorAnalyzer и Server.

FileGen–генерирует файл с параметрами для выбранного технического средства охраны. В зависимости от его типа изменяется число параметров. Значение эталонных параметров можно посмотреть в БД, которая лежит рядом с исполняемым файлом на сервере, в таблице std_params (рис. 4).

std_params | objects

ID	Type	Params_cnt	Params
1	СТВС	2	<40><0,8>
2	СЭНОО	3	<120><50><75,

Рис. 4. Таблица значений с эталонными параметрами

SensorAnalyzer– клиентская часть приложения, которая раз в минуту отправляет параметры из файла на сервер. Server – непосредственно серверная часть разработанной системы. Окно генерации файлов изображено на рис. 5.

В настоящее время многие предприятия нуждаются в автоматизированном простом и быстром средстве контроля технического обслуживания. Предлагаемая «Автоматизированная система контроля обслуживания технических средств охраны систем физической защиты КВО, ПОО», при соответствующем заполнении базы данных может использоваться для контроля состояния технических средств охраны самых любых предприятий, что существенно повысит качество и скорость обслуживания технических средств.

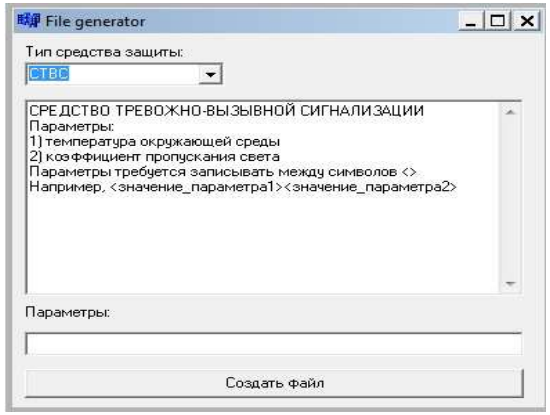

Рис. 5. Генератор файлов

Литература

1. Куделькин В.А., Янников И.М. Структурная схема интеллектуальной интегрированной системы безопасности потенциально опасных объектов //Известия Самарского научного центра Российской академии наук. Том 17, №6(2), – 2015. – С. 726 – 728.

2. Куделькин В.А., Янников И.М. Алгоритм функционирования интеллектуальной интегрированной системы безопасности потенциально опасных объектов // Интеллектуальные системы в производстве № 3 (27) - Ижевск: Изд-во ИжГТУ, 2015. – С. 73 - 76.

3. Янников И.М., Куделькин В.А., Соболева Н.В. Функциональная модель интеллектуальной интегрированной системы безопасности потенциально опасных объектов // Интеллектуальные системы в производстве № 3 (27) - Ижевск: Изд-во ИжГТУ, 2015. – С. 77 - 82.

4. Организация охраны предприятия и физической защиты его объектов http://bezopasnik.org/article/14.htm (Дата обращения: 18.01.2016)

5. Н. В. Давидюк, С. В. Белов Формирование множества характеристик технических средств обнаружения, влияющих на задачу их выбора //Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2009. № 2. – С.110-113.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛЕНИЙ И ТЕЛЕКОММУНИКАЦИИ

Ю.С. Артамонов

ПРОГНОЗИРОВАНИЕ ДОСТУПНЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ КЛАСТЕРА ПРИ ПОМОЩИ МОДЕЛИ EMMSP

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

В области научных вычислений остро стоит вопрос эффективности использования вычислительных ресурсов, поскольку сами ресурсы находятся в дефиците, а исследователи конкурируют за доступ к наиболее производительным окружениям. Под окружением понимается программно-аппаратный комплекс: совокупность физических ЭВМ, каналов связи, периферийных устройств и ПО, необходимого для работы системы. Нередко разработчикам проекта доступно не одно окружение для запуска вычислительных задач, а несколько. В этой ситуации важно грамотно выбрать окружение, в котором вычисления будут завершены как можно раньше.

Подавляющее большинство современных кластеров и суперкомпьютеров используют пакетные системы для запуска задач, а это значит, что каждая задача перед своим запуском проходит через очередь пакетной системы. Время выполнения вычислений в различных окружениях может быть сравнимым, если сами окружения имеют схожую производительность, но время, которое проводит задача в очереди, может отличаться очень сильно, поскольку оно зависит от загруженности окружения и количества запускаемых задач [1]. Кроме того, время ожидания задачи в очереди может быть непредсказуемо для некоторых применяемых политик планирования задач.

Для прогнозирования объёма доступных ресурсов требуются данные о загруженности вычислительных ресурсов и о профиле использования. Под профилем использования понимается набор особенностей окружения, он может быть представлен историческими данными загрузки ресурсов [2]. При прогнозировании следует принять во внимание как большой массив исторических данных по исполнению задач, так и тренд загрузки ресурсов.

Модель прогнозирования EMMSP

Пусть задан временной ряд $Z(t) = Z(1), Z(2), \dots, Z(T)$. Набор последовательных значений $Z_t^M = Z(t), Z(t+1), \dots, Z(t+M-1)$, лежащий внутри исходного временного ряда, назовём выборкой длины M с моментом начала отсчёта t;