4. Газизов Т.Т. Оптимизация генетическими алгоритмами: Учебное методическое пособие [Текст] / Т.Т. Газизов, А.О. Мелкозеров – Томск: кафедра ТУ, ТУСУР, 2006. – 44 с.

С.Г. Пархоменко, Е.В. Симонова

ПОДСИСТЕМА ОЦЕНКИ РИСКОВ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

(Самарский университет)

Введение

Принятие мер с целью обеспечения безопасного и стабильного рабочего процесса является необходимым для каждой организации или предприятия, нацеленного на максимально эффективное осуществление своей деятельности. Одним из современных и действенных подходов к решению данного вопроса, предлагаемых рынком информационной и физической безопасности, является реализация комплексной системы безопасности.

Комплексная система безопасности предприятия – это совокупность программно-аппаратных средств, направленных на охрану и обеспечение безопасности всего предприятия. Консолидируя отдельные подсистемы безопасности (охранно-пожарная сигнализация, система контроля и управления доступом в помещения, видеонаблюдение и т.д.) в монолитную структуру, подобные системы позволяют анализировать и обрабатывать информацию, поступающую с каждой из подсистем, при этом учитывая данные других подсистем. Например, сотрудник службы охраны предприятия, глядя на изображение с системы видеонаблюдения, может удостовериться в личности человека, поднёсшего карту-ключ к электронному считывателю у двери и получившего доступ в помещение.

В ряде случаев с целью повышения уровня защищённости предприятия, снижения вероятности возникновения нештатных ситуаций, обеспечения стабильного рабочего процесса, и как следствие, снижения материальных затрат целесообразно получить общую картину физической безопасности предприятия, а также прогноз относительно аварийных и тревожных ситуаций, которые могут произойти в будущем. На основе прогноза становится возможным оперативное выявление и устранение узких мест в системе безопасности, что позволяет улучшить благосостояние предприятия.

Постановка задачи

Исходя из актуальности и важности вопроса обеспечения и поддержания стабильного исполнения бизнес-процессов на территории организации или предприятия, логичным решением становится реализация механизмов всесторонней оценки текущей ситуации в физической безопасности предприятия, выявления уязвимостей, а также прогнозирования нештатных ситуаций.

Данные механизмы целесообразно объединить и внедрить в комплексную систему безопасности предприятия в виде подсистемы оценки рисков, выполняющей следующие функции:

- мониторинг текущей ситуации в физической безопасности предприятия;
- отслеживание истории изменения состояния системы безопасности, возникновения аварийных и нештатных ситуаций, а также проведённых работ по их устранению;
- адаптация работы под любые изменения в системе безопасности;
- приоритизация выявленных уязвимостей и возможных узких мест в системе безопасности.

Предлагаемое решение

Структурная схема комплексной системы безопасности предприятия представлена на рисунке 1.

Рисунок 1 – Структурная схема комплексной системы безопасности предприятия

К основным узлам системы относятся:

- сервер системы – основной компонент системы, отвечающий за выполнение ключевых функций, необходимых для её работы (обновление конфигураций драйверов устройств, проверка лицензий и т.д.);
- серверы оборудования – один или несколько компьютеров (не ограничено программным способом), к которым выполняется подключение подсистем

безопасности. Число драйверов, обслуживаемых каждым сервером оборудования, ограничивается только производительностью этого сервера [1];

- сервер базы данных – узел, обеспечивающий хранение данных, используемых в процессе работы системы. Для управления данными используется СУБД;
- компьютеры с автоматизированными рабочими местами – неограниченное количество компьютеров с установленными АРМ различного назначения (бюро пропусков, учёт рабочего времени, АРМ оператора и т.д.).

Несколько территориально распределённых объектов, использующих комплексную систему безопасности, могут объединяться с помощью специально предназначенных подсистем [1].

Таким образом, создаётся интегрированная среда обмена сигналами между различными элементами. Все подсистемы работают в комплексе, выполняя одновременно функции контроля, сдерживания, обнаружения опасности, её оценки и реагирования на неё, обеспечивая защиту сразу по нескольким направлениям [2].

Исходя из общей структуры комплексной системы безопасности предприятия, целесообразно распределить работу подсистемы оценки рисков следующим образом: основной функционал подсистемы, представленный выше, выполняется на сервере системы, в то время как управление её работой, а также визуализация результатов оценки рисков осуществляется в одном из клиентских АРМ (логичнее всего АРМ оператора и администратора).

В качестве основного подхода к реализации подсистемы оценки рисков предлагается использование мультиагентных технологий с применением онтологии. В отличие от классического способа, когда проводится поиск некоторого чётко определенного (детерминированного) алгоритма, позволяющего найти наилучшее решение проблемы, с использованием мультиагентных технологий решение получается в результате взаимодействия множества самостоятельных целенаправленных программных модулей – агентов [3].

Одной из ключевых функций подсистемы оценки рисков, описанных выше, является её способность адаптироваться к любым изменениям в системе безопасности. Применение мультиагентного подхода в полной мере позволит удовлетворить данное требование, поскольку одним из свойств, присущих агенту, является его способность к реагированию на изменения в среде.

В качестве инструмента гибкой настройки поведения агентов, а также задания спецификации и конфигурации системы безопасности, принято решение применить онтологии. Онтологии представляют собой концептуальные модели знаний предметной области, которые строятся из наиболее общих понятий (концептов) и отношений между концептами, позволяющих в дальнейшем специфицировать, то есть построить формализованное описание любых объектов или процессов [4]. Как следствие, при появлении новых понятий в системе безопасности (событий, устройств, подсистем и т.д.), их можно будет достаточно легко добавить в онтологию системы безопасности предприятия.

Заключение

Подсистема оценки рисков комплексной системы безопасности предприятия обеспечит действенный инструмент для более эффективной работы как самой системы безопасности, так и предприятия в целом, а технологии, предложенные для её реализации, в полной мере реализуют необходимый функционал подсистемы. Стабильное и безопасное исполнение бизнес-процессов, в конечном итоге, положительно повлияет на бюджет предприятия и на достижение его целей.

Литература

1. Бастион-2. Руководство администратора [Электронный ресурс]. – Режим доступа: URL: http://www.trevog.net/upload/iblock/527/Бастион-2.%20Руководство%20администратора.pdf (дата обращения: 16.03.2018)

2. Комплексные системы безопасности – гарантия стабильной работы и непрерывности бизнес-процессов [Электронный ресурс]. – Режим доступа: URL: https://www.kp.ru/guide/kompleksnye-sistemy-bezopasnosti.html (дата обращения: 16.12.2017)

3. Методологии проектирования мультиагентных систем [Электронный ресурс]. – Режим доступа: URL: https://moluch.ru/conf/tech/archive/228/11320 (дата обращения: 18.03.2018)

4. Онтологии в разработках интеллектуальных систем [Электронный ресурс]. – Режим доступа: URL: http://www.kg.ru/technology/ontology (дата обращения: 18.03.2018)

Д.А. Проценко, Е.В. Симонова

КРИТЕРИИ КАЧЕСТВА ПРОХОЖДЕНИЯ ТРЕНИРОВОК С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ТРЕНАЖЁРА ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ГЛАВНОЙ ОПЕРАТИВНОЙ ГРУППЫ УПРАВЛЕНИЯ ПОЛЁТОМ ИНТЕГРИРОВАННОГО РОССИЙСКОГО СЕГМЕНТА МКС

(Самарский университет)

Введение

Особенностями проведения космических полётов являются постоянный мониторинг систем безопасности жизнедеятельности космонавтов, а также чёткое следование запланированным операциям. В процессе эксплуатации средств Международной космической станции (МКС) существует риск возникновения нештатной (НШС) либо аварийной ситуации (АС), которые требуют незамедлительного реагирования со стороны специалистов Главной оперативной группы управления (ГОГУ) полётом, а также сменного руководителя полётов (СРП).