УДК 681.518.52

И. М. Янников, доктор технических наук, доцент
ИжГТУ имени М. Т. Калашникова
В. А.Куделькин
Консорциум «Интегра-С», г. Самара
М. В. Телегина, доктор технических наук, доцент
ИжГТУ имени М. Т. Калашникова
Т. Г. Габричидзе
Консорциум «Интегра-С», г. Самара

КОМПЛЕКСНЫЙ ПОДХОД К ОРГАНИЗАЦИИ МОНИТОРИНГА ЗАЩИЩЕННОСТИ ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ГИС-ТЕХНОЛОГИЙ

В статье показан разработанный алгоритм получения комплексного описания состояния защищенности территории с использованием геоинформационной системы. Описаны архитектура и функции интеллектуальной системы безопасности «Интегра-4Д», в основу которой положена доменная (кластерная) структура, состоящая из центрального (корневого) и периферийных информационных доменов.

Ключевые слова: геоинформационные системы, серверы и контроллеры безопасности, интегральная система безопасности, домен, кластер.

На сегодняшний день для решения различных задач комплексной безопасности потенциально опасных объектов широко применяются информационные технологии, включающие методы обработки, сбора, анализа, визуализации и поддержки принятия решений.

Особое место в обеспечении безопасности занимают геоинформационные системы (ГИС), обеспечивающие создание единой информационной среды взаимодействия различных взаимоувязанных видов деятельности человека в рамках глобальной системы безопасности и централизованного управления объектами государства. Геоинформационная система обеспечения безопасности – система, обеспечивающая сбор, доступ, отображение и распространение данных о состоянии физической защищенности объекта (объектов).

Геоинформационная интегрированная система безопасности предназначена для использования на объектах в пределах земного шара и обеспечения эффективной комплексной защиты за счет интеграции разрозненных подсистем безопасности. Архитектура системы позволяет полностью контролировать удаленные объекты – получать отчеты и управлять любым устройством в режиме «реального времени». Вся информация хранится и передается в кодированном виде соответствующему третьему уровню секретности.

ГИС безопасности объектов может быть реализована на основе любой инструментальной геоинформационной системы (MapInfo, ArcGIS, WinSTAR, ДубльГИС и другие). ГИС-вьюверы для ГИС безопасности не подойдут, т. к. предоставляют пользователю крайне ограниченные возможности пополнения баз данных. По территориальному охвату различают ГИС: глобальные, субконтинентальные, национальные, региональные, субрегиональные и локальные, или местные [1, 2].

В основу архитектуры ГИС безопасности объектов положена доменная (кластерная) структура, состоящая из центрального (корневого) и периферийных информационных доменов. Каждый кластер более низкого иерархического уровня связан с одним из доменов более высокого уровня, реализуется интегральная оценка безопасности кластера предыдущего иерархического уровня [3].

Средства навигации, определения местоположения объекта и мониторинга его состояния содержат в своем составе высокотехнологичные устройства по сбору информации и ее передаче по каналам связи, базу данных об объектах, которая содержит картографическую информацию и позволяет отображать состояние объекта оператору в реальном времени в удобной форме, а также центры по накоплению и обработке знаний об объектах. Именно такая структура геоинформационной системы соответствует современным требованиям и стандартам, используемым при разработке систем мониторинга и управления сложными организационно-техническими объектами.

В общем виде алгоритм получения комплексного описания состояния защищенности территории с использованием геоинформационной системы приведен на рис. 1.

Начальные три процедуры алгоритма являются подготовительным этапом для работы геоинформационной системы безопасности. В результате их выполнения формируется обновленная карта территории анализируемых объектов.

Определение объектов защиты и их атрибутов

Для обеспечения работы системы безопасности топографическая карта должна быть дополнена необходимыми объектами. В соответствии с нормами и правилами обеспечения физической защищенности объекта это могут быть недостающие объекты, физическую защищенность которых необходимо обеспечивать, и сегменты безопасности (домены, кластеры). Учитывая неполноту существующих баз данных, программа должна предусмотреть добавление в базы данных отсутствующих объектов карты с последующим добавлением сведений об этих объектах (атрибутов).

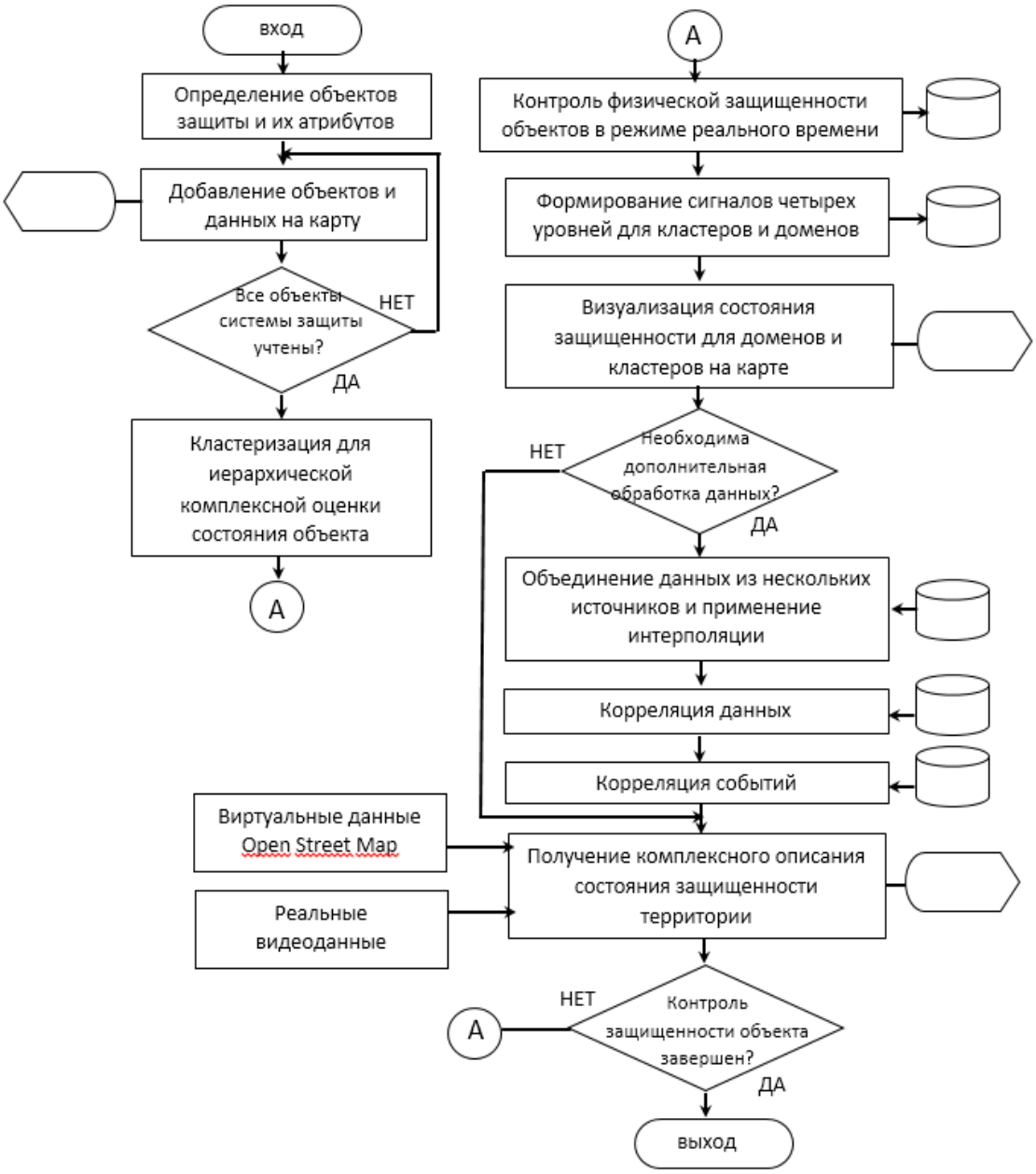

Рис. 1. Алгоритм получения комплексного описания состояния защищенности территории с использованием геоинформационной системы

С целью интеграции существующих баз данных структурных подразделений администрации области, федеральных органов власти Российской Федерации, действующих на территории области, а также предприятий и организаций, владеющих общезначимой информацией, необходима территориальная привязка информации баз данных в геоинформационной системе.

Добавление объектов и данных на карту

Добавляемые объекты (датчики, устройства, объекты, подлежащие охране) на топографической карте могут быть представлены с применением трех видов геометрических примитивов: полигон, линия, точка. Каждому объекту карты соответствует определенный набор атрибутов (числовые или символьные характеристики).

Для отображения пространственных данных по контролируемым объектам необходима топографическая карта соответствующего масштаба и наполнения. Чтобы не использовать незаконно созданную картографическую продукцию и с целью необходимости интеграции данных с государственным цифровым картографическим фондом предлагается нормативным образом ввести в практику использование единой топографо-геодезической основы цифровых карт всеми организациями вне зависимости от их ведомственной принадлежности.

Кластеризация для иерархической комплексной оценки состояния объекта подразумевает формирование доменов и кластеров карты разного иерархического уровня. Домен – это сегмент безопасности, отображающий состояние группы кластеров более низкого иерархического уровня. В рамках топогра-

фической карты домен представляет собой полигональный объект, на территории которого расположены кластеры (группа датчиков). В качестве атрибутов доменов будет кроме информации о территориальной и ведомственной принадлежности объектов (регионов и т. д.) информация о состоянии датчиков, устройств низшего уровня иерархии [4].

Кластер – группа датчиков, расположенных в пределах одного объекта. Кластер отвечает на периферии за датчик, группу датчиков или устройств безопасности объекта или его подразделений.

Серверы низшего уровня соединены через контроллеры безопасности с цифровыми датчиками безопасности.

Контроль физической защищенности объектов в режиме реального времени состоит из сбора данных с различных датчиков физической безопасности объекта. При работе датчики безопасности, установленные на объектах, передают информацию о состоянии безопасности объекта через контроллеры безопасности на серверы низшего уровня. При этом для оценки текущего состояния датчиков применена специальная система кодирования (в общем случае и уровней угроз системы безопасности).

Для обеспечения мониторинга территориально распределенных объектов производства, транспорта и прилегающей территории предусматривается создание унифицированных образцов в целях осуществления интеллектуального видеонаблюдения уязвимых элементов, обнаружения опасных веществ, контроля транспортной и инженерной инфраструктуры, подсистем ЖКХ, систем обеспечения жизнедеятельности, метеорологической и экологической обстановки, рис. 2 [5, 6].

Рис. 2. Контроль действующих транспортных объектов

Формирование сигналов четырех уровней для кластеров

Как отмечено ранее, в качестве пространственно-временных атрибутов кластеров может быть использована информация с датчиков, характеризующая состояние физической защищенности объекта. Система ИИСБ содержит серверы нескольких уровней безопасности, соединенных между собой при помощи каналов связи через сеть Интернет и глобальную систему навигации. Сбор информации о состоянии безопасности объекта осуществляется с датчиков, установленных на объектах.

Информация о контролируемых объектах поступает на соответствующие уровни принятия решений от диспетчерского пункта объекта до национального центра мониторинга и управления государством, автоматизировано распределяется в соответствии с полномочиями и обязанностями пользователей и сложившейся в государстве иерархией управления.

Производится их передача на серверы низшего уровня с последующим анализом и передачей наиболее важной информации на серверы более высокого уровня. Наиболее важная информация от датчиков передается на серверы 2 второго уровня.

Формирование сигналов четырех уровней для доменов

Из подсистем мониторинга локальных систем жизнеобеспечения объектов в геоинформационную систему на сервер 1 высшего уровня поступает значительно меньший объем информации, но имеющий большую значимость:

(0) – нормальное состояние;

(1) – ненормальная работа (сбои, отказы устройств, наладка);

(2) – опасность первого уровня (устраняемая на региональном уровне);

(3) – глобальная опасность.

Передача информации на вышестоящий уровень сопровождается интегральной оценкой безопасности кластера (набора связанных объектов) с пометкой соответствующим цветом. При этом передается только необходимая информация, фильтруемая по степеням важности специальными алгоритмами.

Уполномоченное лицо с любого терминала (компьютер, планшет, смартфон) имеет доступ к разрешенным ресурсам системы, защищенным электронной подписью и механизмом шифрации, сертифицированным ФСБ и ФСТЭК России.

Мониторинг системы может осуществляться с любого мобильного устройства: ноутбук, смартфон, планшет (рис. 3) [7]. Защита данных производится шифрацией по ГОСТ 28147–89 (256 бит) с использованием сертифицированного соответствующими службами оборудования и программного обеспечения (VipNet).

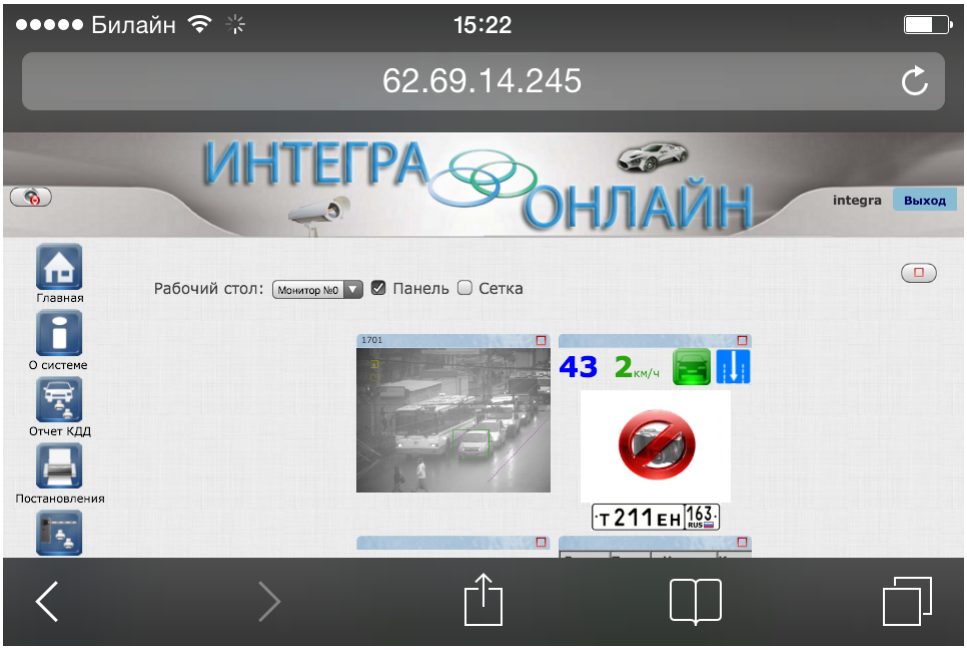

Рис. 3. Интерфейс доступа в систему безопасности с помощью мобильного устройства

Визуализация состояния защищенности для доменов и кластеров на карте

Особенностью отображения данных о физической защищенности потенциально опасных объектов в геоинформационной системе безопасности является применение 4D-изображений с возможностью интеграции, управления и анализа пространственно-временных данных от различных систем.

Из подсистем мониторинга (технологических процессов, сетей ЖКХ и т. д.), локальных систем жизнеобеспечения объектов в геоинформационную систему поступает постоянно только необходимая информация в виде двоичных кодов, сопровождаемая цветовыми оценками состояния объектов.

Объединение данных из нескольких источников и применение интерполяции (расчета промежуточных значений, кадров) необходимо для получения развернутой информации для оценки ситуации на объекте. Проводиться может как оценка текущей ситуации, так и оценка обстановки на контролируемых объектах за прошлые периоды мониторинга.

Корреляция данных – это объединение однотипного оборудования (схожих датчиков, камер или устройств) одного объекта для иерархической комплексной оценки состояния объекта: неисправности, тревоги, запрос обслуживания, что снижает количество ложных тревог.

Корреляция событий определяет разнородные события и уведомляет оператора, что они могут быть связаны, это помогает игнорировать отвлекающие факторы и определить угрозы безопасности.

Отображение всех устройств системы и их связей в виде иерархического дерева необходимо для наглядности взаимных связей устройств и использования автоматического и ручного формирования базы данных устройств, программирования логических связей по линиям передачи данных, питания и т. д.

Инструменты поддержки принятия решений (инциденты) призваны помочь оператору системы при выполнении различных задач во время инцидента, увеличивая скорость и эффективность работы, автоматически отображая связанные с ними видеофайлы и события системы.

Разработанная и программно реализованная в соответствии с приведенным алгоритмом интеллектуальная система безопасности «Интегра-4Д» разработана на основе принципов открытых систем с целью упрощения интеграции с другими системами. «Интегра-Планета-4Д» содержит открытые программные интерфейсы для интеграции с источниками информации и внешними информационными системами [8].

Библиографические ссылки

1. *Телегина М. В.* Геоинформационные системы и основы дешифрирования : учеб. пособие / сост. М. В. Телегина. – Ижевск : Изд-во ИжГТУ, 2012. – 160 с.

2. Геоинформационные системы и экологическое картографирование : учеб. пособие / сост. М. В. Телегина, И. М. Янников. – Ижевск : Изд-во ИжГТУ, 2012 – 156 с.

3. Интегра-Планета-4D. – URL: http://www.msu.ru/entrance (дата обращения: 18.09.2015).

4. Кризис предупреждения чрезвычайных ситуаций и пути его преодоления : учебно-практическое пособие / В. В. Артяков, А. В. Болтовский, Т. Г. Габричидзе, А. М. Зайцев, В. А. Куделькин, Т. Г. Лебедева и др. ; под ред. д-ра техн. наук Т. Г. Габричидзе. – 3-е изд., испр. И доп. – Самара : Изд-во СамНЦ РАН, 2015. – 266 с.

5. Там же.

6. *Куделькин В. А*. О преимуществах для построения системы видеонаблюдения на транспорте // Системы безопасности. – № 1 (121). – С. 127.

7. *Куделькин В. А.* Удаленный терминал интегрированной интеллектуальной системы // Патент на полезную модель №: 45036. Патентообладатель ЗАО «ВОЛГАСПЕЦРЕМСТРОЙ» ; опубл. 10.04.2005.

8. Распоряжение Правительства Российской Федерации от 17 декабря 2010 г. № 2299-р и по ГОСТ Р 22.1.12–2005, п. 5.1.

* * *

Yannikov I. M., DSc in Engineering, Associate Professor, Kalashnikov ISTU
Kudelkin V. A., Consortium "Integra-S", Samara
Telegina M.V., DSc in Engineering, Associate Professor, Kalashnikov ISTU
Gabrichidze T. G., Consortium "Integra-S", Samara

Integrated approach to security monitoring of potentially hazardous objects using GIS technology

The paper presents the algorithm for obtaining a comprehensive description of the state of protected areas using geographic information systems. It describes the architecture and features of the intelligent security system "INTEGRA-4D", which is based on a domain (cluster) structure consisting of a Central (root) and peripheral information domains.

Keywords: geoinformation systems, server and security controllers, integrated security system domain, cluster.

Получено: 30.10.15