УДК 004:504.05
DOI 10.22213/2410-9304-2017-4-94-101

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

ОСОБЕННОСТИ ОБРАБОТКИ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНОЙ ИНТЕГРИРОВАННОЙ СИСТЕМЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ И ТЕРРИТОРИЙ

В работе представлена интеллектуальная интегрированная система безопасности, предназначенная для обеспечения комплексной безопасности объектов и территорий и представляющая собой сложный программно-технический комплекс, состоящий из различных подсистем безопасности и мониторинга. Приведены основные принципы создания и практические подходы к построению системы. На основе вышеуказанных принципов впервые сформулированы принципы создания интегрированных систем безопасности (ИИСБ) КВО и ПОО, легшие в основу Единых требований к проектированию и созданию интегрированных систем безопасности в виде комплекса технических средств, предназначенных для управления различными устройствами ИИСБ. Данные требования, обладающие информационной, технической, эксплуатационной и программной совместимостью, легли в основу ГОСТ Р 56875–2016 «Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий».

Поскольку практическая реализации системы безопасности на объектах и территориях во многом зависит от компетентности информированности должностных лиц, имеющих отношение к вопросам обеспечения безопасности, в целях решения данной проблемы авторами статьи предлагается ряд положений – практических подходов к построению интеллектуальной интегрированной системы безопасности ИИСБ-4D. Данные подходы послужили основой для разработки очередного проекта ГОСТ РФ «Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов, предприятий и территорий. Архитектура и общие технические требования к оборудованию и программным средствам интегрированных систем обеспечения безопасности», прошедшего окончательную экспертизу в техническом комитете и направленного на утверждение в Росстандарт РФ.

В статье приведен широкий перечень научной, методической и нормативно-правовой литературы, необходимой для практической реализации систем безопасности на объектах и территориях.

Ключевые слова: интеллектуальная интегрированная система безопасности, геоинформационная система, системы управления доступом, видеонаблюдение, кроссплатформенное приложение, датчики, мониторинг, критически важные и потенциально опасные объекты, отчеты, визуализация, кластеризация, корреляция.

В последние годы с ростом научно-технического прогресса и резкого ухудшения природно-климатической и экологической обстановки все большую актуальность приобретает проблема обеспечения безопасного функционирования критически важных и потенциально опасных объектов (КВО и ПОО), являющихся, как правило, сложными организационно-техническими и технологическими системами. В создавшихся условиях обеспечить безопасность указанных объектов можно лишь путем создания соответствующих научно-технических разработок комплексных систем безопасности и их практической реализации как в области оценки влияния КВО и ПОО на окружающую среду, так и в области обеспечения комплексной безопасности указанных объектов [1, 2].

На наш взгляд, при постановке задач обеспечения комплексной безопасности критически важных и потенциально опасных целесообразно проведение следующих мероприятий [3]:

– оценки возможности и определения инструментов интеграции организационных, методических и технических средств обеспечения безопасности на различных уровнях управления;

– разработки функционально-полной архитектуры комплексов средств безопасности объектов с повышенными рисками угроз безопасности, позволяющей проектными методами обеспечить «встраивание» компонентов систем безопасности различных производителей в действующие организационно-технические системы управления объектами;

– разработки общих требований к оборудованию и программному обеспечению интегрированных систем безопасности объектов и территорий, позволяющих обеспечить производство необходимых сертифицированных средств на российских предприятиях для снижения зависимости от импорта.

Иными словами, для обеспечения комплексной безопасности объектов и территорий долж-

на быть разработана и практически реализована интегрированная интеллектуальная система безопасности (ИИСБ), предназначенная для решения следующих основных задач [4]:

1. Обеспечение мониторинга территориально распределенных муниципальных образований и субъектов РФ (интеллектуальное видеонаблюдение уязвимых элементов, обнаружение опасных веществ, контроль транспортной и инженерной инфраструктуры, систем обеспечения жизнедеятельности, метеорологической и экологической обстановки, их сопряжения с органами повседневного управления РСЧС различных уровней).

2. Автоматическое получение, сбор, передача информации (отображения) для контроля за текущей обстановкой, на объектах ее изменения, прогнозирования для органов управления и реагирования на них.

3. Автоматизированная выработка рекомендаций по организации и реализации комплекса оперативных контрольно-проверочных, силовых, режимных и других мер в случае возникновения событий и ситуаций, требующих вмешательства со стороны органов повседневного управления РСЧС.

4. Автоматизированная информационно-аналитическая поддержка деятельности органов управления и должностных лиц всех уровней при управлении мероприятиями в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера.

5. Создание единого информационного пространства интегрированной интеллектуальной системы безопасности на территории опасных объектов, в муниципальных образованиях и субъектах Российской Федерации.

Разработанная интеллектуальная интегрированная система безопасности (ИИСБ-4D) [5–9], объединившая все подсистемы безопасности и мониторинга в единую 4D-геоинформационную систему, предоставляет ситуационный анализ территорий и объектов (с отображением инцидентов и возможностью просмотра изменений ситуации во времени и пространстве на многослойных 3D-картах).

Подсистема отображения ИИСБ-4D, представляющая собой кроссплатформенное приложение в виде единого четырехмерного мира, интегрирует пространственно-временные данные, поступающие от различных систем (СОПС, СКУД, СВН, АИС и др.), а также управляет ими и анализирует. При необходимости любые системы – поставщики аналитической информации, могут быть интегрированы через интерфейс прикладного программирования (ИПП) и систему подключаемых модулей (СПМ) (в том числе радиационный, химический, биологический, экологический, технологический и другие виды мониторинга).

Информационные и аналитические системы представлены системами: паспортного контроля, контроля автотранспорта, контроля движения, а также прочими системами природного, технологического, экологического и иного контроля окружающей среды.

Размещаемые в виртуальном пространстве объекты привязаны к географическим координатам, масштабированы и могут иметь различную степень детализации.

В подсистеме отображения реализована технология дополненной виртуальной реальности (ДВР), представляющей собой видеоизображение, «наложенное» на объекты трехмерного виртуального мира. Это позволяет более полно воспринимать информацию (видеть одновременно расположение видеокамеры в трехмерном пространстве и поступающее с нее видеоизображение) (рисунок).

В целях повышения эффективности существующих систем предлагается использование следующих методов:

– *объединение данных* из нескольких источников и применение методов интерполяции для получения развернутой информации;

– *корреляцию данных,* объединяющую схожие датчики или камеры одного объекта и, как следствие, снижающую количество ложных тревог;

– *корреляцию событий*, определяющую сами события и уведомляющую оператора о их взаимосвязи с целью игнорирования отвлекающих факторов и более четкого определения реальных угроз;

– *кластеризацию*, объединяющую однотипное оборудование для иерархической комплексной оценки состояния объекта (неисправности, тревоги, запрос обслуживания);

– *разработку схемы*, отображающей все устройства системы и их связи в виде иерархического дерева (автоматическое и ручное формирование базы данных устройств, программирование логических связей по линиям передачи данных, питания и т. д.);

– *интерактивное руководство* – пошаговые процедуры управления рабочим процессом с возможностью взаимодействия с системами онлайн-техподдержки (видеозаписи действий с целью последующего анализа);

– *создание специальных слоев* – вопросы компетенции секретного (служебного) пользования, рассматриваемые исключительно на определенном рабочем месте;

– *использование закладок*, позволяющих системным операторам помечать событие и связанные с ним данные датчиков, камер или нарушения правил доступа;

– *процедуру выявления и реагирования на инциденты* с использованием инструментов поддержки принятия решений «ИИСБ-4D», помогающих оператору системы при выполнении различных задач во время происшествия (увеличение скорости работы, автоматически отображение нужных видеороликов и временных событий).

Наложение видеоизображения на объекты трехмерного виртуального мира

В отличие от большого количества существующих в стране разрозненных систем безопасности указанная платформа, построенная на строго научном, системном подходе, доказала свою высокую технологичность и надежность. Она способна обеспечивать надлежащую защиту объектов и территорий нашей страны от различных рисков, в том числе угроз террористического характера.

На основе анализа концептуальной модели обеспечения комплексной безопасности КВО и ПОО авторами сформулированы принципы создания интегрированных систем безопасности [10]:

1. *Принцип системности,* предполагающий наличие комплекса взаимосвязанных элементов динамической системы, взаимодействующей с внешней средой (угрозы, автоматическая защита, организационные решения) при этом объекты системы получают новые свойства, направленные на повышение защищенности объекта.

2. *Принцип единства информации,* предполагающий использование единой терминологии, способов представления данных, условных обозначений и т. д., принятых соответствующими нормативными документами отраслевого значения. Ситуационный анализ территорий и объектов на многослойных картах с возможностью отображения инцидентов позволит не только своевременно выявлять угрозы, но и служить базой для принятия наиболее оптимальных решений.

3. *Принцип иерархичности,* предполагающий, что ИИСБ должна строиться как многоуровневая иерархическая система с принятием автоматических и управленческих решений, с передачей информации на разные иерархические уровни с использованием принципов вертикальной и горизонтальной интеграции [11].

4. *Принцип свертки информации,* предполагающий использование передачи «укрупненной информации» при движении по ступеням иерархии снизу вверх.

5. *Принцип постоянного контроля,* предполагающий возможность получения информации в любом месте и в любое время, при доступности относительно простой схемы установки, управления и программирования, оперативного контроля за системами жизнеобеспечения объектов и зданий. Для этого предполагается использование кроссплатформенных программных компонентов ИИСБ, открытых программных интерфейсов и каналов беспроводной связи Интернет, стандарта GSM и Wi-Fi. При интеграции технических и программных средств необходимо выполнение защиты всех данных и

видеофайлов электронной подписью (при хранении на сервере и при передаче).

6. *Принцип инвариантности* предусматривает требования к использованию стандартных компонентов систем безопасности: технических и программных средств, что способствует снижению затрат при создании ИИСБ.

В соответствии с предложенными принципами сформулированы основные требования к оборудованию и программному обеспечению ИИСБ объектов и территорий [12–14], легшие в основу Государственного стандарта Российской Федерации «Информационные технологии системы безопасности комплексные и интегрированные» [15].

Как правило, практическая реализация этой системы на объектах и территориях во многом зависит от компетентности и должной информированности должностных лиц, имеющих отношение к вопросам обеспечения безопасности. В целях решения данной проблемы предлагается ряд положений – практических подходов к построению интеллектуальной интегрированной системы безопасности ИИСБ-4D.

Подходы к построению интеллектуальной интегрированной системы безопасности ИИСБ-4D.

1. *Работа под управлением операционной системы (ОС) с открытыми исходными кодами (Linux и др.)*. Исходный код таких систем доступен для просмотра и изменения, что позволяет пользователю не только контролировать работу самой программы, но и принимать участие в ее доработке, корректировке, создании новых программ. Данная система делает невозможной скрытую установку разведывательного или вредоносного программного обеспечения и исключает возможность утечки информации, поскольку открытый исходный код исключает наличие закладок.

ОС с закрытыми исходными кодами (например, ОС Windows, iOS, MacOS американских корпораций) делает систему незащищенной и уязвимой со стороны обладателей исходного кода [16]. Действующая законодательная и нормативно-правовая база запрещает использование всех программ иностранного производства в российских государственных и муниципальных учреждениях [17–20].

2. *Использование открытых протоколов обмена данными устройств и программных продуктов* позволяет интегрировать программное обеспечение и оборудование разных производителей в единый аппаратно-программный комплекс (АПК), концепция построения и развития которого утверждена распоряжением Правительства Российской Федерации [21], а единые требования к техническим параметрам его сегментов – приказом МЧС России [22]. Указанные документы являются правовой основой интеграции систем.

3. *Визуализация состояния объектов и территорий в 3D-ГИС-исполнении с привязкой компонентов системы мониторинга (видеокамер, датчиков, контроллеров и др.) к пространственным координатам и времени* позволяет вести мониторинг объектов, размещенных на различных уровнях, в том числе и подземных, простым клик-приказом на точку карты-схемы, получая на экране изображения камер, в зоне действия которых находится интересующее место. Привязка всех компонентов системы безопасности на 3D-плане объекта с отражением их функционального состояния повышает оперативность устранения возможных технических отклонений в ее работе [23–25].

4. *Шифрование передаваемых данных до степени секретности объекта* осуществляется во исполнение требований российского законодательства [26] и обеспечивает защиту информации.

5. *Применение электронной подписи (ЭП)* обеспечивает санкционированный доступ к информации и, как следствие, защиту от несанкционированного доступа, персональную ответственность за целостность и достоверность передаваемой информации и ее искажение (дезинформацию) [27–29].

6. *Полицентрическое построение системы безопасности* предполагает, что информация анализируется, обрабатывается и хранится непосредственно на объектах или органах управления (распределенных центрах), а не в едином центре. При этом передача событий осуществляется всем пользователям одновременно (в соответствии с правами доступа к каналам передачи информации). Нарушение работы части системы или отдельных каналов не приводит к потере информации и утрате работоспособности всей системы, а следовательно, обеспечивает ее устойчивость в соответствии с требованиями ГОСТ Р 56875–2016.

7. *Интеграция* с органами повседневного управления РСЧС позволяет собирать, обрабатывать и предоставлять оперативную информацию для принятия решений при угрозе или возникновении ЧС природного, техногенного или террористического характера.

В данном контексте существенна поддержка протокола отраслевого стандарта ONVIF версии

не ниже 2.2, который дополнительно определяет спецификации веб-сервисов и соответствующие требования по доступу к ним в рамках протоколов XML / SOAP / HTTP в части:

– получения сведений о медиаисточниках (видеокамерах, аудио-, фотоисточниках), в том числе об их географическом местоположении и областях обзора видеокамер;

– импорта медиазаписей в форме файлов, в том числе с привязкой к координатам места записи постоянных данных (для стационарных источников) и изменяющихся во времени (геотреки для мобильных источников);

– ограничения доступа к медиаисточникам с разбивкой по типу взаимодействия – получения «живых»/«архивных» медиаданных, управления PTZ, фокусировкой видеокамер и др.;

– управления заданиями на выполнение длительных операций, например отслеживания транспортного средства (его поиска на фото / видеоизображениях по регистрационному номеру).

Данные подходы послужили основой для разработки проекта Государственного стандарта «Интегрированные интеллектуальные системы мониторинга и обеспечения безопасности распределенных объектов, предприятий и территорий. Архитектура и общие технические требования к оборудованию и программным средствам интегрированных систем обеспечения безопасности». Проект прошел окончательную экспертизу в техническом комитете и направлен на утверждение в Росстандарт РФ.

Подытоживая вышеизложенное, отметим, что приведенные принципы и подходы позволяют осуществить поэтапную интеграцию существующих и вновь создаваемых систем мониторинга, а также наращивать их возможности на базе единого технологического фундамента – «Интеллектуальной интегрированной системы безопасности ИИСБ-4D».

Библиографические ссылки

1. *Габричидзе Т. Г., Янников И. М.* Структура и принцип построения комплексной многоступенчатой системы безопасности КВО (ХОО, ОУХО) // Теоретическая и прикладная экология. 2007. № 2. С. 55–69.

2. *Телегина М. В., Янников И. М., Габричидзе Т. Г.* Методы и алгоритмы оценки воздействия потенциально опасных объектов на окружающую среду : монография. Самара : Изд-во Самар. НЦ РАН, 2011. 200 с.

3. *Куделькин В. А., Денисов В. Ф.* Интегрированные интеллектуальные системы мониторинга и обеспечения комплексной безопасности городов. URL: http://daily.sec.ru (дата обращения: 24.09.2017 г.).

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

5. Там же.

6. *Янников И. М., Куделькин В. А., Телегина М. В., Габричидзе Т. Г.* Комплексный подход к организации мониторинга защищённости потенциально опасных объектов с использованием ГИС-технологий // Интеллектуальные системы в производстве. 2015. № 3 (27). С. 83–87.

7. *Куделькин В. А., Янников И. М.* Алгоритм функционирования распределенной разноуровневой интеллектуальной системы безопасности потенциально опасных объектов // Интеллектуальные системы в производстве. 2015. № 3 (27). С. 73–76.

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

9. *Янников И. М., Соболева Н. В., Куделькин В. А., Казанцев М. М., Габричидзе Т. Г.* База данных средств физической защиты потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15, № 1. С. 122–125.

10. *Куделькин В. А., Янников И. М., Телегина М. В.* Принципы создания интегрированных систем безопасности критически важных и потенциально опасных объектов // Интеллектуальные системы в производстве. 2017. Т. 15, № 1. С. 105–109.

11. Анализ уязвимости объекта (общие положения). 2013. 5 июля [Электронный ресурс] // Сайт ЗАО НПП «ИСТА-Системс» (г. Санкт-Петербург). URL: http://ista-systems.ru/ (дата обращения: 27.10.2015).

12. ИНТЕГРА-С. Интеллектуальные системы безопасности. ТК-22 «Информационные технологии» (ПК-125) [Электронный ресурс] // Сайт Консорциума «Интегра-С» (г. Самара). URL: http://www.integra-s. com/company/tk22/ (дата обращения: 14.10.2015).

13. *Куделькин В. А.* Безопасный город – безопасное государство! // Системы безопасности. 2014. № 4 (118). С. 129.

14. *Куделькин В. А., Бахрах Г.* Как решает проблемы обслуживания ИСБ компания «Интегра-С» // Системы безопасности. 2014. № 1 (115). С. 91.

15. Государственный стандарт Российской Федерации ГОСТ Р 56875–2016 «Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий».

16. Терроризм – угроза обществу : учеб.-метод. пособие / под ред. В. А Куделькина и С. А. Савкиной. Самара : Изд-во СамНЦ РАН, 2017. 464 с.

17. Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о

защите информации» (в ред. от 29 июня 2015 ФЗ № 188).

18. Федеральный закон № 44 от 05.04.2013 г. «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (в ред. от 29 июня 2015 ФЗ № 188).

19. Постановление Правительства РФ от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

20. План перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011–2015 годы. Утв. распоряжением Правительства РФ от 17 декабря 2010 года № 2299-р.

21. Распоряжение Правительства Российской Федерации от 3 декабря 2014 года № 2446-р.

22. Временные единые требования к техническим параметрам сегментов. Приказ МЧС России 29 декабря 2014 г. № 14-7-5552.

23. Распоряжение Правительства РФ от 17 ноября 2008 года № 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года».

24. Рекомендации по созданию трехмерных геоизображений (моделей) территорий и объектов жизнеобеспечения, потенциально-опасных, критически важных для национальной безопасности. Утверждены МЧС России 25 февраля 2009 года № 2-4-60-3-28.

25. Технические требования к программно-техническим комплексам структурированных систем мониторинга и управления инженерными системами зданий и сооружений (СМИС) объектов, сопрягаемым с органами повседневного управления РСЧС (муниципального и территориального уровней). Утверждены МЧС России 9 сентября 2011 года № б/н.

26. Федеральный закон от 21 июля 1993 г. года № 5485-1 «О государственной тайне».

27. Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

28. Приказа Минкомсвязи России от 13 апреля 2012 года № 107 «Об утверждении Положения о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», зарегистрированного в Минюсте России 26 апреля того же года за № 23952».

29. ГОСТ Р 56875–2016 «Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий», утвержденного и введенного в действие приказом Росстандарта от 26 февраля 2016 г. № 81-ст.

References

1. Gabrichidze T. G., Jannikov I. M. (2007). *Teoreticheskaja i prikladnaja jekologija* [Theoretical and Applied Ecology], no. 2, pp. 55-69 (in Russ.).

2. Telegina M. V., Jannikov I. M., Gabrichidze T. G. (2011). *Metody i algoritmy ocenki vozdejstvija potencial'no opasnyh ob#ektov na okruzhajushhuju sredu* [Methods and algorithms for assessing the impact of potentially hazardous objects on the environment]. Samara: Samar. NC RAN (in Russ.).

3. Kudel'kin V. A., Denisov V. F. *Integrirovannye intellektual'nye sistemy monitoringa i obespechenija kompleksnoj bezopasnosti gorodov* [Integrated intelligent systems for monitoring and ensuring integrated urban security], available at http://daily.sec.ru (accessed September 24, 2017).

4. Kudel'kin V. A., Jannikov I. M. (2015). *Izvestija Samarskogo nauchnogo centra Rossijskoj akademii nauk* [Izvestiya Samara Scientific Center of the Russian Academy of Sciences], vol. 17, no. 6 (2), pp. 726-728 (in Russ.).

5. Ibid.

6. Jannikov I. M., Kudel'kin V. A., Telegina M. V., Gabrichidze T. G. (2015). *Intellektual'nye sistemy v proizvodstve* [Intellectual systems in production], no. 3 (27), pp. 83-87 (in Russ.).

7. Kudel'kin V. A., Jannikov I. M. (2015). *Intellektual'nye sistemy v proizvodstve* [Intellectual systems in production], no. 3 (27), pp. 73-76 (in Russ.).

8. Jannikov I. M., Kudel'kin V. A., Soboleva N. V. (2015). *Intellektual'nye sistemy v proizvodstve* [Intellectual systems in production], no. 3 (27), pp. 77-82 (in Russ.).

9. Jannikov I. M., Soboleva N. V., Kudel'kin V. A., Kazancev M. M., Gabrichidze T. G. (2017). *Intellektual'nye sistemy v proizvodstve* [Intellectual systems in production], vol. 15 no. 1, pp. 122-125 (in Russ.).

10. Kudel'kin V. A., Jannikov I. M., Telegina M. V. (2017). *Intellektual'nye sistemy v proizvodstve* [Intellectual systems in production], vol. 15 no. 1, pp. 105-109 (in Russ.).

11. *Analiz ujazvimosti ob"ekta (obshhie polozhenija). 2013. 5 ijulja* [Analysis of the vulnerability of the object (general provisions). 2013. July 5]. Sajt *ZAO NPP «ISTA-Sistems» (g. Sankt-Peterburg)* [The site of ZAO NPP ISTA-Systems (St. Petersburg)], available at http://ista-systems.ru/ (accessed October 27, 2015).

12. *INTEGRA-S. Intellektual'nye sistemy bezopasnosti. TK-22 «Informacionnye tehnologii» (PK-125)* [INTEGRA-S. Intelligent security systems. TK-22 "Information Technologies" (PK-125)]. *Sajt Konsorciuma «Integra-S» (g. Samara)* [The site of the Integra-S Consortium (Samara)], available at http://www.integra-s.com/company/tk22 (accessed October 14, 2015).

13. Kudel'kin V. A. (2014) *Sistemy bezopasnosti* [Security systems], no. 4 (118), p. 129 (in Russ.).

14. Kudel'kin V. A., Bahrah G. (2014) *Sistemy bezopasnosti* [Security systems], no. 1 (115), p. 91 (in Russ.).

15. *Informacionnye tehnologii sistemy bezopasnosti kompleksnye i integrirovannye. Tipovye trebovanija k arhitekture i tehnologijam intellektual'nyh sistem monitoringa dlja obespechenija bezopasnosti predprijatij i territorij*, GOST R 56875–2016 (Information technologies of the security system are integrated and integrated. Typical requirements for the architecture and technologies of intelligent monitoring systems for ensuring the security of enterprises and territories) (in Russ.).

16. Kudel'kin V. A., Savkinoj S. A. (id.) (2017) *Terrorizm – ugroza obshhestvu* [Terrorism is a threat to society]. Samara: Izd-vo SamNTs RAN (in Russ.).

17. *Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii*, Federal'nyi zakon № 149-FZ ot 27.07.2006 [Information, information technologies and information protection] (in redaction June 29, 2015, FZ № 188) (in Russ.).

18. *O kontraktnoi sisteme v sfere zakupok tovarov, rabot, uslug dlya obespecheniya gosudarstvennykh i munitsipal'nykh nuzhd*, Federal'nyi zakon № 44 ot 05.04.2013 [About contract system in the sphere of procurement of goods, works, services for provision of state and municipal needs] (in redaction June 29, 2015, FZ № 188) (in Russ.).

19. *Ob ustanovlenii zapreta na dopusk programmnogo obespecheniya, proiskhodyashchego iz inostrannykh gosudarstv, dlya tselei osushchestvleniya zakupok dlya obespecheniya gosudarstvennykh i munitsipal'nykh nuzhd*. Postanovlenie Pravitel'stva RF ot 16 noyabrya 2015 goda № 1236 [On the establishment of a ban on the admission of software originating from foreign countries, for the purpose of procurement for the provision of state and municipal needs] (in Russ.).

20. *Plan perekhoda federal'nykh organov ispolnitel'noi vlasti i federal'nykh byudzhetnykh uchrezhdenii na ispol'zovanie svobodnogo programmnogo obespecheniya na 2011–2015 gody* [The plan for the transition of federal executive bodies and federal budget institutions to the use of free software for 2011-2015]. Approved Decree of the Government of the Russian Federation of December 17, 2010, no. 2299-r (in Russ.).

21. *Rasporyazhenie Pravitel'stva Rossiiskoi Federatsii ot 3 dekabrya 2014 goda № 2446-r* [Decree of the Government of the Russian Federation of December 3, 2014 No. 2446-r] (in Russ.).

22. *Vremennye edinye trebovaniya k tekhnicheskim parametram segmentov*, Prikaz MChS Rossii 29 dekabrya 2014 g. № 14-7-5552 [Temporary unified requirements for technical parameters of segments] (in Russ.).

23. *O Kontseptsii dolgosrochnogo sotsial'no-ekonomicheskogo razvitiya Rossiiskoi Federatsii na period do 2020 goda*, Rasporyazhenie Pravitel'stva RF ot 17 noyabrya 2008 goda № 1662-r [On the Concept of Long-Term Social and Economic Development of the Russian Federation for the Period to 2020] (in Russ.).

24. *Rekomendatsii po sozdaniyu trekhmernykh geoizobrazhenii (modelei) territorii i ob"ektov zhizneobespecheniya, potentsial'no-opasnykh, kriticheski vazhnykh dlya natsional'noi bezopasnosti* [Recommendations for the creation of three-dimensional geoimages (models) of territories and life support facilities, potentially dangerous, critical for national security], approved by the Ministry of Emergency Situations of Russia on February 25, 2009, no. 2-4-60-3-28 (in Russ.).

25. *Tekhnicheskie trebovaniya k programmno-tekhnicheskim kompleksam strukturirovannykh sistem monitoringa i upravleniya inzhenernymi sistemami zdanii i sooruzhenii (SMIS) ob"ektov, sopryagaemym s organami povsednevnogo upravleniya RSChS (munitsipal'nogo i territorial'nogo urovnei)* [Technical requirements for software and hardware systems of structured systems for monitoring and managing engineering systems of buildings and structures (MISC) of facilities, which are interfaced with the bodies of day-to-day management of the RSES (municipal and territorial levels)], approved by the EMERCOM of Russia on September 9, 2011, no. б/н (in Russ.).

26. *O gosudarstvennoi taine*, Federal'nyi zakon ot 21 iyulya 1993 g. goda № 5485-1 [On State Secrets] (in Russ.).

27. *Ob elektronnoi podpisi*, Federal'nyi zakon ot 6 aprelya 2011 goda № 63-FZ [About the electronic signature] (in Russ.).

28. *Ob utverzhdenii Polozheniya o federal'noi gosudarstvennoi informatsionnoi sisteme «Edinaya sistema identifikatsii i autentifikatsii v infrastrukture, obespechivayushchei informatsionno-tekhnologicheskoe vzaimodeistvie informatsionnykh sistem, ispol'zuemykh dlya predostavleniya gosudarstvennykh i munitsipal'nykh uslug v elektronnoi forme», zaregistrirovannogo v Minyuste Rossii 26 aprelya togo zhe goda za № 23952*, Prikaza Minkomsvyazi Rossii ot 13 aprelya 2012 goda № 107 [On approval of the Regulation on the federal state information system "Unified system for identification and authentication in the infrastructure providing information and technological interaction of information systems used to provide state and municipal services in electronic form" registered with the Ministry of Justice of Russia on April 26 of the same year for No. 23952] (in Russ.).

29. *Informatsionnye tekhnologii. Sistemy bezopasnosti kompleksnye i integrirovannye. Tipovye trebovaniya k arkhitekture i tekhnologiyam intellektual'nykh sistem monitoringa dlya obespecheniya bezopasnosti predpriyatii i territorii,* GOST R 56875-2016 [Information Technology. Security systems are integrated and integrated. Typical requirements for the architecture and technologies of intelligent monitoring systems for ensuring the security of enterprises and territories], approved and put into effect by order of Rosstandart on February 26, 2016 No. 81-st (in Russ.).

* * *

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

Data Processing Features in the Intellectual Integrated Security System of Objects and Territories

The work presents an intelligent integrated security system designed to provide complex security of objects and territories and is a complex software and hardware complex consisting of various security and monitoring subsystems. The main principles of creation and practical approaches to the system construction are given. Based on the above principles for the first time, the principles for the creation of integrated security systems (IISS) for CWE and VET, formed the basis for the Unified Requirements for the Design and Development of Integrated Security Systems in the Form of a Complex of Technical Means for Managing Various IISB Devices. These requirements, which have information, technical, operational and software compatibility, formed the basis of the Standard GOST R 56875-2016 "Complex and integrated information technologies for security systems. Typical requirements for the architecture and technologies of intelligent monitoring systems for ensuring the security of enterprises and territories".

Since the practical implementation of the security system in the objects and territories depends to a large extent on the competence of the information security officials, in order to solve this problem, the authors of the paper propose a number of provisions - practical approaches to the construction of the intellectual integrated safety system IISB-4D. These approaches served as the basis for the development of the next draft of the Standard GOST of the Russian Federation "Integrated intelligent monitoring and security systems for distributed objects, enterprises and territories. Architecture and general technical requirements for the hardware and software of integrated security systems", which passed the final examination in the technical committee and was sent to Rosstandart for approval.

The paper lists a wide range of scientific, methodological and legal literature necessary for practical implementation of security systems at sites and territories.

Keywords: intelligent integrated security system, geoinformation system, access control systems, video surveillance, cross-platform application, sensors, monitoring, critical and potentially dangerous objects, reports, visualization, clustering, correlation.

Получено: 17.10.17