УДК 681.51(045)
DOI: 10.22213/2410-9304-2017-1-105-109

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

ПРИНЦИПЫ СОЗДАНИЯ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ И ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

На основе обобщенной классификации угроз, воздействующих на цели защиты, показано, что система комплексной безопасности должна функционировать как единая система управления, контроля и мониторинга возможных опасностей. Среди недостатков существующих подходов к построению интегрированных систем безопасности (ИСБ) выделены разрозненность существующей методологической базы к проектированию и реализации ИИСБ и автоматизации выдачи рекомендуемых решений, а также отсутствие единых требований к системам безопасности.

С целью повышения физической защищенности критически важных и потенциально опасных объектов (ПОО и КВО) предлагается использовать интеллектуальную интегрированную систему безопасности (ИИСБ), которая характеризуется непрерывным мониторингом по сбору, обработке, документированию (архивированию), передачей информации в едином информационном поле.

На основе анализа концептуальной модели обеспечения комплексной безопасности КВО и ПОО сформулированы принципы создания интегрированных систем безопасности: принцип системности, принцип единства информации, принцип иерархичности, принцип свертки информации, принцип постоянного контроля, принцип инвариантности.

Ключевые слова: критически важные и потенциально опасные объекты, интегрированные интеллектуальные системы безопасности, принципы построения, системный подход.

В последние годы все большую обеспокоенность вызывает состояние критически важных и потенциально опасных объектов (КВО и ПОО) в связи с постоянно усиливающимся антропогенным прессингом на окружающую среду и, как следствие, увеличением количества и масштабов природных катаклизмов. Кроме того, усиливается рост международной напряженности и особенно террористических проявлений. Вполне понятно, что вышеуказанные объекты, обеспечивающие устойчивое функционирование экономики в условиях чрезвычайных ситуаций, должны быть надежно защищены от любых внешних воздействий. Но ПОО и сами по себе являются сложными инженерно-техническими сооружениями, функционирование которых сопряжено с риском возникновения аварий и чрезвычайных ситуаций (ЧС) [1–5].

Аварии на ПОО характеризуются достаточно широким набором поражающих факторов: механических (взрывная волна, разрушение конструкций); термических (воздействие пониженной или повышенной температур); электроэнергетических (воздействие электрического тока); радиационных (воздействие ионизирующих излучений); химических (воздействие отравляющих веществ); биологических (воздействие патогенных микроорганизмов) и др.

Обобщенная классификация угроз, воздействующих на цели защиты, приведена на рис. 1. Виды угроз, воздействующие на цели защиты, образуют общее для данного КВО или ПОО пространство угроз. Каждая из угроз при этом, независимо от цели воздействия, по своим последствиям носит комплексный характер.

Поскольку воздействие негативных факторов на объекты носит комплексный характер, то системы их защиты тоже должны быть комплексными.

Система комплексной безопасности должна функционировать как единая система управления, контроля и мониторинга возможных опасностей, вследствие чего должна включать в свою структуру как минимум несколько подсистем (рис. 2) [6].

К принципам построения системы комплексной безопасности КВО и ПОО следует отнести: принцип законности (с учетом действующего законодательства); системности (выявление и учет всех взаимосвязанных и взаимодействующих элементов, компонентов, условий и факторов, существенно значимых для формирования системы предупреждения и ликвидации ЧС); адаптивности (возможность внесения изменений в структуру системы в зависимости от обстановки); непрерывности (безопасность должна осуществляться на всех стадиях функционирования ПОО от проектирования до вывода из эксплуатации); совместимости (организационная, технологическая и информационная совместимость всех компонентов и элементов системы); приемлемый уровень риска (обеспечение уровня риска обеспечивающего безаварийное функционирование объекта); предупреждения (приоритет предупреждения самого факта ЧС перед мерами по снижению возможных последствий) [7].

Рассматривая вопросы защищенности ПОО и КВО, необходимо отметить, что подсистема их физической безопасности также должна носить комплексный характер, обусловленный прежде всего комплексным воздействием негативных факторов, оказывающих влияние на ПОО. Она должна быть интегрированной (сопряженной с другими подсистемами безопасности указанных объектов и соответствующими сторонними подсистемами) и носить многоуровневый, многофункциональный характер.

Существующие в настоящее время подходы к построению интегрированных систем безопасности (ИСБ) имеют ряд существенных недостатков, основными из которых являются: разрозненность сущест-

вующей методологической базы к проектированию и реализации ИИСБ и автоматизации выдачи рекомендуемых решений, а также отсутствие единых требований к системам безопасности, что приводит к разнообразию и, как следствие, невозможности сопряжения программно-аппаратных комплексов и оборудования. Все это резко снижает эффективность указанных систем.

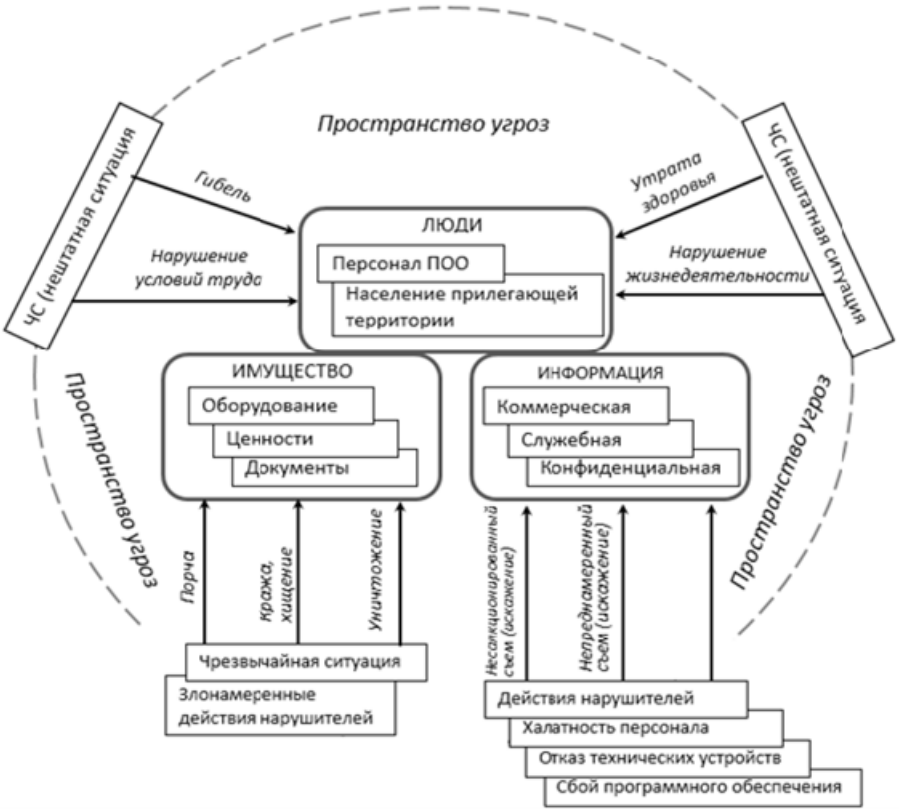

Рис. 1. Цели защиты в пространстве угроз

Рис. 2. Элементы системы комплексной безопасности

Системный подход к построению интегрированных интеллектуальных систем безопасности (ИИСБ), в том числе к созданию методологической базы их проектирования и реализации, а также автоматизация выдачи рекомендуемых решений позволят учитывать все взаимосвязи в структуре объекта между системами безопасности, технологическим оборудованием, системами жизнеобеспечения и, следовательно, оптимальным образом по критериям эффективность – стоимость обеспечить защиту объекта.

С целью повышения физической защищенности ПОО и КВО предлагается использовать интеллекту-

альную интегрированную систему безопасности (ИИСБ), которая характеризуется непрерывным мониторингом по сбору, обработке, документированию (архивированию), передачей информации в едином информационном поле. Создание интегрированной системы безопасности основывается на индивидуальных специфических свойствах объекта физической защиты. Проектирование системы безопасности должно учитывать все его особенности: характеристики помещений, инженерно-технических систем, ограждающих конструкций, их соответствия нормативно-технической документации (СНИП, ГОСТ и прочие), требования обеспечения безопасности.

На основе анализа концептуальной модели обеспечения комплексной безопасности КВО и ПОО сформулируем принципы создания интегрированных систем безопасности:

1. *Принцип системности.* Части интегрированной системы безопасности представляют собой комплекс взаимосвязанных элементов, образующих некоторую целостность. Они образуют открытую динамическую систему, активно взаимодействующую с окружающей средой (угрозы, нарушения, автоматическая защита, организационные решения). Объекты, объединенные в систему, получают новые свойства: уменьшение вероятности реализации угроз, в том числе и комбинированного характера, и, как следствие, повышение защищенности объекта.

2. *Принцип единства информации.* В широком смысле он предполагает использование единой терминологии, способов представления данных, условных обозначений и т. д., принятых соответствующими нормативными документами отраслевого значения. Для систем безопасности это будут единые способы представления информации – отображение объектов на 2D- или 3D-плане местности в 3D-изображении самого объекта с размещением всех систем безопасности и контроля с привязкой к географическим координатам. Поэтому ИИСБ должна иметь возможность импорта картографических данных из общепринятых обменных форматов ГИС. Объединение всех систем в единую 4D-информационную систему с получением видеоданных в реальном масштабе времени обеспечит получение наглядной и оперативной информации.

Ситуационный анализ территорий и объектов на многослойных картах с возможностью отображения инцидентов не только позволит своевременно выявлять угрозы, но и будет служить базой для принятия адекватных обстановке и наиболее оптимальных решений.

3. *Принцип иерархичности.* Система безопасности должна строиться как многоуровневая иерархическая система с принятием соответствующих автоматических и управленческих решений и дальнейшей передачей информации на разные иерархические уровни. Для объединения через формирование различного типа связей между субъектами, проявляющихся в различном соединении их ресурсов систем безопасности, необходимо сочетание и развитие принципов вертикальной и горизонтальной интеграции.

Вертикальная интеграция – в системах управления безопасностью ПОО и КВО подразумевает связь между разноуровневыми системами сбора, обработки, анализа информации принятия решений посредством вертикальных информационных потоков. Иерархическая сетевая структура, на которой основаны современные информационные системы, включает в себя различные компьютерные и локальные сети различных уровней сложности специализированных вычислительных устройств.

Горизонтальная интеграция – объединение на аппаратно-программной платформе различных типов подсистем (охранная сигнализация, пожарная сигнализация, контроль доступа, видеонаблюдение, управление инженерными системами и др.). Аппаратно-программмная платформа может состоять из оборудования разных производителей в рамках одной подсистемы [8].

4. *Принцип свертки информации*. Для выполнения на каждом уровне иерархии всего комплекса мер по защите объектов предлагается использовать передачу «укрупненной информации» при движении по ступеням иерархии снизу вверх. Для того чтобы на верхнем уровне иерархии успешно решались стратегические задачи, необходима информация, достаточно полно описывающая те параметры ситуации, которые определяют стратегические решения, и «не замусоренная» второстепенными подробностями, на решение существенно не влияющими.

5. *Принцип постоянного контроля*. Подразумевается возможность получения информации в любом месте и в любое время как при наличии диспетчерской, так и в случае, когда диспетчерская отсутствует вовсе (абсолютно автономное функционирование ИИСБ). Должна быть обеспечена доступность и относительно простая схема установки, управления и программирования; оперативный контроль за системами жизнеобеспечения объектов и зданий.

С целью интеграции с источниками информации и внешними информационными системами предлагается использовать кроссплатформенные программные компоненты ИИСБ, открытые программные интерфейсы и работу под управлением операционных систем с открытым исходным кодом. С этой целью необходимо использование каналов беспроводной связи Интернет стандарта GSM и Wi-Fi.

По степени открытости передаваемая информация чаще всего может быть ограниченного уровня доступа, поэтому при интеграции технических и программных средств необходимо выполнение защиты всех данных и видеофайлов электронной подписью (при хранении на сервере и при передаче). С терминала, имеющего доступ к сети Интернет, доступ уполномоченному лицу к разрешенной информации, защищенной электронной подписью и механизмом шифрации, также должен быть защищен электронной подписью.

6. *Принцип инвариантности* предусматривает требования к использованию стандартных компонентов систем безопасности: технических и программных средств, что способствует снижению за-

трат при создании ИИСБ. Предлагается использование стандартных промышленных технических средств (датчиков, барьеров…), программных средств – геоинформационных систем, протоколов передачи данных, механизмов защиты информации и т. п.

На основании этих принципов создаются интегрированные системы безопасности в виде комплекса технических средств, предназначенных для управления различными устройствами комплексной безопасности, обладающими информационной, технической, эксплуатационной и программной совместимостью.

В соответствии с предложенными принципами основные требования к оборудованию и программному обеспечению ИИСБ объектов и территорий можно сформулировать следующим образом [9–11]:

1. Все программные компоненты интеллектуальных ИСБ должны быть кроссплатформенными и работать под управлением операционных систем с открытым исходным кодом.

2. Интегрированная интеллектуальная система безопасности (ИИСБ) должна разрабатываться на основе принципов открытых систем с целью упрощения интеграции с другими системами ИИСБ, содержать открытые программные интерфейсы для интеграции с источниками информации и внешними информационными системами.

3. ИИСБ должна иметь возможность импорта картографических данных из общепринятых обменных форматов. (Примеры общепринятых форматов – «Шейп-файл» (Shapefile), Sxf и т. д.).

4. Объекты должны отображаться на 2D- или 3D-плане местности в 3D-изображении самого объекта с размещением всех систем безопасности и контроля с привязкой к географическим координатам. Объединение всех систем безопасности в единую 4D-информационную систему представляет собой ситуационный анализ территорий и объектов на многослойных 3D-картах с возможностью отображения инцидентов.

5. Электронной подписью должны быть защищены все данные и видеофайлы (при хранении на сервере и при передаче). Доступ уполномоченному лицу к разрешенной информации, защищенной электронной подписью и механизмом шифрации, с терминала, имеющего доступ к сети Интернет, также должен быть защищен электронной подписью.

Таким образом, предложены единые правила к проектированию и реализации ИИСБ КВО и ПОО, обеспечивающие возможность их сопряжения в единую систему безопасности объектов и территорий.

Данные технические требования, разработанные в соответствии с предложенными принципами построения ИИСБ, изложены в 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».

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. Принципы комплексного управления безопасностью территорий / В. А. Алексеев, А. П. Кузнецов, В. А. Назаров, Т. Г. Габричидзе, П. М. Фомин, И. М. Янников // Интеллектуальные системы в производстве. – 2008. – № 2 (12). – С. 120–127.

3. К вопросу определения понятия комплексной системы безопасности / В. А. Алексеев, В. А. Власов, Т. Г. Габричидзе, П. М. Фомин, Б. А. Якимович, И. М. Янников // Технологии гражданской безопасности. – 2008. – №3 (17). – С. 17–19.

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

5. Комплексная многоступенчатая система безопасности критически важных, потенциально опасных объектов : монография / Т. Г. Габричидзе, В. А. Власов, А. Ю. Кудрин, В. А. Алексеев, П. М. Фомин, И. М. Янников, Б. А. Якимович. – Ижевск : Научная книга, 2007. – 184 с.

6. *Янников И. М., Прокофьев Д. В.* Комплексная безопасность потенциально опасных объектов. Предпосылки и принципы ее построения // Математические модели и информационные технологии в организации производства. – 2015. – № 1(30). – С. 35–38.

7. Там же.

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

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

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

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

* * *

V. A. Kudel'kin, Senior Lecturer, Consortium "Integra-S", Samara
I. M. Yannikov, DSc in Engineering, Associate Professor, Kalashnikov ISTU
M. V. Telegina, PhD in Engineering, Associate Professor, Kalashnikov ISTU

Principles of Developing the Integrated Security Systems of Critical and Potentially Dangerous Objects

On the basis of the generalized classification of threats affecting the target's defense, it is shown that the integrated security system should function as a unified system of management, control and monitoring of possible threats. Among the shortcomings of existing approaches to the construction of integrated security systems (ISS) the fragmentation is highlighted for the existing methodological frame-

work for the design and implementation of the IISS and the automation of presenting the recommended solutions, as well as the lack of uniform safety system requirements.

In order to improve the physical security of critical and potentially dangerous objects, it is proposed to apply an intelligent integrated security system (IISS), which is characterized by continuous monitoring of the collection, processing, filing (archiving), and transmission of information in a single information field. Based on the analysis of the conceptual model to ensure the comprehensive security of critical and potentially dangerous objects, the principles of integrated safety systems are formulated: the system principle, the principle of unity of information, the principle of hierarchy, the principle of data convolution, the principle of continuous monitoring, and the invariance principle.

Keywords: Critically important and potentially hazardous objects, integrated intelligent safety systems, principles of development, system approach.

Получено: 30.01.17