УДК 654.924

ОСНОВНЫЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ

В.В. Волхонский

На основе общего подхода к проблеме обеспечения безопасности анализируются основные угрозы и риски для защищаемых объектов. Сформулированы общие принципы построения объединенных интегрированных систем обеспечения безопасности объектов и перечень исходной информации, необходимой для разработки таких систем, а также рассмотрены вопросы оценки прямой и косвенной экономической эффективности системы.
Ключевые слова: угрозы, риски, безопасность, интегрированная система.

Введение

Одним из важнейших вопросов при построении системы безопасности (СБ) является разработка концепции обеспечения безопасности, определяющая все основные характеристики разрабатываемой СБ. В большинстве публикаций задача разработки такой концепции привязана либо к конкретному типу обо-

рудования, либо к конкретному объекту. Это априорно снижает функциональные возможности разрабатываемой системы и увеличивает риски. Кроме того, зачастую разработка систем ведется вообще без разработки концепции и детального анализа возможных угроз, а только на основе типового решения с определенными функциональными возможностями. Это приводит к тому, что не учитывается целый ряд угроз и возможных потерь для объекта. В работе предпринята попытка сформулировать в общем виде основные положения концепции обеспечения безопасности, применимые для различных объектов и оборудования разных производителей. На основе анализа формулируются базовые требования к объединенным интегрированным системам безопасности (ОИСБ), решающим задачу обеспечения безопасности в широком смысле.

Основные понятия и определения

Общее понятие безопасности, жизненно важных интересов и объектов безопасности определено в Законе РФ [1]. Более узкие понятия противокриминальной и антитеррористической охраны и безопасности определены в Национальном стандарте РФ [2].

В работе предлагается общий подход к проблеме построения СБ, охватывающий не только вопросы противокриминальной и антитеррористической охраны и безопасности, но и многие другие стороны обеспечения безопасности в самом широком смысле. Иначе говоря, рассмотрены не только традиционные направления обеспечения безопасности, включающие средства охранной и пожарной сигнализации, ТВ наблюдения, контроля и управления доступом, но другие направления. К последним можно отнести системы жизнеобеспечения зданий и сооружений (кондиционирование, вентиляция, отопление и др.); энергосбережение, т.е. анализ потребляемых ресурсов (холодная и горячая вода, электроэнергия, газ и т.д.); мониторинг местоположения на объекте персонала, важного имущества, средств транспорта и т.п.; контроль работоспособности технологического оборудования, а также и любые другие направления так или иначе связанные с безопасностью. Упомянутые направления в настоящее время контролируются, как правило, независимо от «традиционных» СБ. Усложнение криминогенной обстановки и, в первую очередь, рост террористической угрозы требуют более общего единого подхода. Связь упомянутых направлений непосредственно с безопасностью достаточно очевидна. К примеру, состояние воздушной среды (обычно контролируемое системой инженерных коммуникаций здания или вообще не контролируемое) непосредственно влияет на безопасность находящихся в этом здании людей. Надо также понимать, что угрозы могут быть не только прямыми, но и опосредованными. А опосредованные угрозы зачастую легче реализовать, если не предусмотрены их обнаружение и соответствующая реакция на них СБ. Например, искусственное задымление в системе вентиляции здания, где проводятся массовые мероприятия, может привести к давке с очень серьезными последствиями. Общий подход должен предусматриваться не только на этапе разработки структуры СБ, но и на всех остальных этапах, начиная от анализа угроз и заканчивая обслуживанием и модернизацией системы.

С этой точки зрения в работе будут использоваться следующие более общие понятия. Субъект или объект обеспечения безопасности (СООБ) – жизнь, здоровье, окружающая среда, имущество и информация. Безопасность – состояние защищенности СООБ от различных угроз. Система безопасности (СБ) – совокупность методов и средств предупреждения, обнаружения, противодействия развитию и ликвидации угроз жизни, здоровью, окружающей среде, имуществу и информации. Угроза – факторы (события, действия, процессы и т.п.), приводящие к возможности возникновения ситуации, при которой происходит нарушение состояния защищенности СООБ. Риск – возможность реализации угрозы, приводящей к тому или иному уровню потерь (ущерба) для СООБ.

Перечень угроз для задачи построения противокриминальной и антитеррористической СБ, как правило, включает такие угрозы, как пожар, кража, нападение, терроризм, вандализм, несанкционированный доступ. Однако с безопасностью в широком смысле связаны и многие другие угрозы, например, утечка воды или жидкостей, приводящих к материальным потерям; утечка газов (непосредственно создающих угрозу СООБ или приводящих к возникновению других угроз, например, пожара или взрыва); ухудшение состояния воздушной среды (недопустимый уровень загрязнения или изменения температурного режима и т.п.); неисправность технологического оборудования, создающая угрозы; угрозы, создаваемые для СООБ самой ОИСБ, например, средствами автоматизированного пожаротушения; человеческий фактор (защита «от дурака», подкуп или запугивание, паническое поведение толпы и т.п.), а также многое другое. Задача обнаружения и ликвидации таких угроз может и должна решаться в единой системе. Очевидно, что решение проблемы обеспечения безопасности в широком смысле возможно только при использовании именно ОИСБ, включающей как технические и программные средства «традиционных» направлений обеспечения безопасности, так и другие, реализующие защищенность от перечисленных выше угроз.

Таким образом, только комплексное решение всех вопросов единой ОИСБ позволит обеспечить максимальную эффективность системы с точки зрения обнаружения различных угроз и своевременную реакцию на ту или иную угрозу.

Эффективность ОИСБ будет также зависеть и от ряда других вопросов. Например, разработка структуры системы и состава оборудования без учета вопросов эксплуатации в дальнейшем может сни-

жать не только экономическую эффективность СБ, но и функциональную. Необходим также единый подход и на всех этапах создания и эксплуатации ОИСБ.

Угрозы и риски

Анализ, выполняемый на основе полного перечня угроз и учитывающий оценки вероятностей реализации угроз и возможного ущерба от их реализации, позволяет составить перечень реальных (с высокой вероятностью реализации) и существенных (приводящих к существенным потерям) угроз, учитываемых при разработке ОИСБ.

Естественно, при этом должны приниматься во внимание все возможные ограничения, в частности, экономические, юридические (законодательные), организационные, технические и другие, в той или иной степени важные в решаемой задаче.

Упомянутые выше угрозы могут при необходимости группироваться в такие основные категории, как криминальные, террористические, техногенные, природные, субъективные и др. Такая группировка может позволить правильно составить полный перечень возможных угроз. При этом надо понимать, что некоторые угрозы могут входить в часть или во все группы. Например, пожар может возникнуть как результат поджога (криминал или терроризм), неисправности электропроводки или оборудования (техника), небрежности человека (субъект) или молнии (природное явление). В связи с этим также необходимо конкретизировать возможные способы реализации каждой угрозы.

Можно говорить о следующих основных видах рисков: реализации угроз, возникновения потерь для СООБ при реализации угрозы и безнаказанности выполнения несанкционированных действий, а также о рисках, связанных непосредственно с процессом разработки и реализации самой ОИСБ [3, 4] и, в конечном итоге, влияющих на безопасность собственно СООБ – технический (возможность отказа СБ); непредсказуемый (непредсказуемое развитие ситуации); осознанный (сознательный отказ от обеспечения безопасности того или иного приоритета); заданный (взятый за основу возможный риск и уровень последствий реализации угроз) и системный (связанный с угрозами, создаваемыми СБ при ее функционировании и во внештатных ситуациях).

Общие принципы построения СБ

Разработка концепции построения объединенных интегрированных систем безопасности может основываться на следующих базовых принципах.

- Решение задачи обеспечения безопасности объекта в широком смысле, с учетом всех составляющих, необходимых для эффективного обеспечения противокриминальной, антитеррористической, антивандальной, технологической, информационной, экономической, экологической и других направлений обеспечения безопасности субъекта или объекта, необходимых в каждой конкретной задаче. В ряде случаев упомянутые составляющие могут перекрываться, например, противокриминальная защита также решает часть вопросов антитеррористической и информационной безопасности. Однако в разных случаях конечная цель преступника, методы его действий и используемые им средства могут существенно отличаться и, как следствие, требовать различных средств и методов обеспечения безопасности. Например, цель кражи (материальная выгода) достигается, если преступник не только достиг цели, но и вышел за пределы досягаемости сил реагирования. Если он был задержан на месте совершения кражи или даже после нее, то потери, как правило, минимальны и приемлемы. Однако террористу-смертнику этого не требуется – достижение им цели уже позволяет реализовать теракт, и потери могут быть катастрофические.
- Реализация полностью интегрированного решения упомянутых выше задач в комплексе на всех этапах построения системы: анализа объекта и всех его особенностей; анализа всех возможных угроз, оценки вероятности их реализации и возможных потерь при реализации и составления списка реальных угроз; проектирования системы; монтажа оборудования; пусконаладочных работ; обучения персонала СБ на начальном этапе и поддержания уровня квалификации в процессе эксплуатации; обучения персонала объекта; обслуживания системы в процессе эксплуатации; модернизации СБ (программного обеспечения и оборудования, расширения СБ и т.д.).
- Учет, по возможности, всех реальных угроз (прямых, опосредованных, первичных, вторичных), приводящих к существенным потерям для СООБ.
- Оценка вероятности реализации угроз и возможных потерь от реализации угроз, а также уровней допустимых потерь.
- Оценка рисков и возможных потерь от реализации самой ОИСБ.
- Решение упомянутых выше задач в оптимальном, соответствующем задаче и требованиям заказчика смысле. Иначе говоря, наиболее эффективном с функциональной, экономической, технической, вероятностной и других точек зрения.

– Разработка комплекса организационных мероприятий по реагированию на нештатные ситуации персонала службы безопасности и самого объекта.

Основные исходные данные

Очевидно, что в каждой конкретной задаче список исходных данных будет различаться и зависеть от особенностей объекта и режима его функционирования. Однако в общем случае исходные данные могут быть следующие.

– Общая структура объекта, включающая в себя: перечень групп объектов или комплексов, входящих в состав объекта обеспечения безопасности и территориально разнесенных между собой (например, комплекс спортивных сооружений – горнолыжный комплекс, стадион, каток и т.д.); состав и функциональное назначение объектов в каждой группе; конструктивные особенности каждого объекта. Территориальное расположение объектов на местности с учетом особенностей рельефа, растительности, других близлежащих объектов и коммуникаций; наличие и характеристики водных объектов (море, озеро, каналы, водоводы, речки и т.п.), находящихся в непосредственном контакте с ООБ, т.е. пересекающие объект или граничащие с ним; социальные, этнические и религиозные особенности региона.
– Транспортная инфраструктура объекта, включающая следующие основные элементы: каждодневные способы доставки персонала и посетителей в эти группы объектов (железнодорожный, автомобильный транспорт и т.д.; с разделением по персоналу, посетителям и обслуживанием) из мест их нахождения (например, спортсменов из олимпийской деревни, зрителей из мест проживания); разовые способы транспортировки персонала и посетителей на период различных массовых мероприятий, непосредственно перед мероприятием и после; количество постоянно находящихся на объекте жителей, персонала фирм и т.п.; ориентировочное каждодневное количество посетителей (максимальное, изменение количества во времени и в календарные периоды и т.д.).
– Основные средства жизнеобеспечения этих объектов (кабельные или воздушные ЛЭП, каналы поставки продуктов, воды, теплоснабжения и т.п.).
– Каналы связи, которые используются непосредственно для целей обеспечения режима функционирования объектов, их защищенность, возможности их использования для СБ, возможность использования специальных каналов связи для СБ и т.п.
– Материалы уже имеющиеся в распоряжении заказчика, такие как следующие: технические требования к системе и ее элементам; организационные требования к режиму работы системы; ведомственные и иные требования к ОИСБ; анализ угроз, рисков и уязвимостей, уже сделанный заказчиком.
– Ограничения на зону ответственности разработчиков ОИСБ, в частности, необходимость учета таких задач, как обеспечение безопасности от подготовки терактов на этапе строительства; защиты информации, в частности, каналов связи; защита средств жизнеобеспечения этих объектов, расположенных вне самих объектов; контроль поставок продуктов питания, напитков и т.п.; обеспечение безопасности водных акваторий (над- и подводных); обеспечение безопасности воздушного пространства; обеспечение режима безопасности на окружающей территории и господствующих высотах и т.п.

Ясно, что невозможно учесть заранее все особенности объектов. В связи с этим в каждом конкретном случае вышеприведенный перечень может расширяться и дополняться в зависимости от поставленных требований и ограничений.

Основные требования к системе безопасности

ОИСБ должна строиться на основе общих базовых принципов, изложенных выше. Непрекращающаяся дискуссия о том, какая из подсистем безопасности должна быть основой для интегрированной системы безопасности, вряд ли имеет серьезный смысл. Она продиктована главным образом желанием производителя продвинуть именно свое оборудование и программные средства. В каждом конкретном случае решение должно приниматься в зависимости от поставленной задачи. Если наиболее важными являются функции, к примеру, охранной сигнализации, то и брать за основу обычно лучше программное обеспечение этой подсистемы. Но главный принцип построения ОИСБ – единая общая платформа интеграции всех подсистем, необходимых для решения задачи обеспечения комплексной безопасности конкретного объекта с возможностью в дальнейшем эффективных модернизации и развития программного и аппаратного обеспечения системы. Это обеспечивается предъявлением следующих основных требований к ОИСБ.

Проектные

– Обоснованность всех используемых подсистем и элементов разрабатываемой ИСБ.
– Адекватность структуры, состава и стоимости системы угрозам, рискам и возможным потерям.
– Соответствие требованиям государственных стандартов и ведомственных документов.

Структурные

– Многоуровневая архитектура обнаружения угроз и принятия решения.

- Программная и аппаратная масштабируемость системы.
- Программная и аппаратная модульность построения системы.
- Пространственно-распределенная архитектура.
- Централизованное и децентрализованное управление подсистемами.

Функциональные

- Решение задач предупреждения угроз (поддержание безопасного состояния).
- Многофункциональность подсистем (возможность выполнения подсистемами не только своих основных функций, но и части функций других подсистем).
- Обнаружение угроз с учетом требований максимально раннего обнаружения (по возможности, на этапе подготовительных или начальных действий) и максимально надежного обнаружения за счет использования высоконадежных средств обнаружения; соответствия их принципов обнаружения характеру проявления угроз; обнаружения одних и тех же угроз на основе различных физических принципов обнаружения; обнаружения одних и тех же угроз разными подсистемами для повышения вероятности обнаружения системой в целом; интегрального принятия решения на основе использования комплекса информации от устройств обнаружения всех подсистем.
- Самодиагностика и самоконтроль ОИСБ с автоматическим выявлением не только и самих неисправностей, но и возможности их возникновения.
- Защищенность самой СБ от несанкционированных действий, таких как маскирование и блокирование средств обнаружения угроз, вскрытия элементов системы, нарушения каналов связи, съема информации о системе, попыток несанкционированного изменения ее параметров и т.п. действий.
- Инвариантность СБ к изменениям окружающей среды и условий взаимодействия с другими элементами объекта и самой системы.
- Резервирование всех основных жизненно важных элементов системы.
- Инвариантность к типу каналов связи и возможность их дублирования с использованием различных физических принципов действия.

Организационные

- Возможность своевременного и максимально эффективного реагирования на угрозу для минимизации возможных потерь.
- Возможность высокой степени адаптации (аппаратной, программной, организационной, функциональной) к особенностям объекта и режиму его функционирования.
- Открытость для использования оборудования и программных средств различных производителей оборудования.

Информационные

- Высокая информативность устройств обнаружения угроз.
- Высокая степень автоматизации процессов обработки информации и принятия решения в системе для снижения влияния человеческого фактора.
- Применение типовых протоколов обмена (LonWorks, BACnet, OPC, …).
- Интеграция с приложениями, используемыми на объекте (PeopleSoft, SAP, …).

Кроме того, с точки зрения непосредственно режима функционирования ОИСБ должна удовлетворять основным требованиям, сформулированным в работе [3].

Эффективность системы

Комплексный подход к разработке ОИСБ подразумевает также и комплексный подход к оценке затрат на создание и эксплуатацию системы, т.е. учет стоимости всех этапов построения СБ (анализ объекта, проектирование, поставка оборудования, монтаж, пуско-наладка, обучение персонала, обслуживание, расширение, модернизация). Это позволяет минимизировать затраты в комплексе при достижении максимальной эффективности работы системы в целом. Очевидно, что в общем случае должны учитываться различные стороны эффективности:

- функциональная (возможность решения всех поставленных задач обеспечения комплексной безопасности объекта);
- техническая (надежная система с эффективным использованием своих ресурсов);
- экономическая, включающая в себя следующее:
  - прямую эффективность, т.е. экономию на содержании и обучении персонала службы безопасности; за счет минимизации количества персонала СБ (операторов, обслуживающего персонала, ...); путем энергосбережения (рационального использования различных ресурсов, расходуемых объектом обеспечения безопасности, таких как электроэнергия, вода, газ, пар, топливо и т.п.); за счет максимально рационального использования служб реагирования (благодаря уменьшению количества ложных тревог в системе); на уменьшении эксплуатационных расходов на систему; на снижении расходов на модернизацию системы; на снижении расходов на расширение системы (как аппаратное, так и функциональное); уменьшение страховых взносов и выплат;

– косвенную эффективность, обеспечиваемую за счет таких показателей, как оптимизация отношения цена/качество; уменьшение уровня рисков; возможность получения всех видов услуг из одних рук; достижение максимальной непрерывности бизнеса и, как следствие, обеспечение репутации надежной компании; удобство модернизации СБ за счет совместимости оборудования и программных средств; удобство количественного и функционального расширения СБ за счет гибкой структуры платформы интеграции; повышение уровня автоматизации обработки информации; повышение удобства обслуживания; обеспечение интеграции с другими подсистемами предприятия; обеспечение многофункциональности системы; обеспечение эффективной интеграции и взаимодействия различных подсистем; реализация единого управления всеми подсистемами; обеспечение оптимального рабочего климата для достижения максимальной производительности труда; минимизация количества нештатных ситуаций, влияющих на непрерывность бизнеса (за счет предупреждения, раннего обнаружения и проверки правильности обнаружения нештатной ситуации); минимизация последствий (потерь) от нештатных ситуаций.

Различные способы оценки того или иного вида эффективности приведены в ряде опубликованных работ, например, в [4].

Заключение

На основе представленного подхода были разработаны концепции обеспечения безопасности и реализованы системы безопасности для различных по сложности и функциональным особенностям государственных и коммерческих объектов в Российской Федерации и странах СНГ. Предложенный подход является достаточно общим и позволяет на его основе в каждом конкретном случае эффективно решить конкретную задачу. Эффективность реализации изложенной концепции подтверждается длительным успешным опытом эксплуатации упомянутых СБ.

Литература

1. Закон Российской Федерации от 5 марта 1992 г. №2446-1 «О безопасности» (в редакции 07.03.2005).
2. ГОСТ Р 52551-2006. Национальный стандарт Российской Федерации. Термины и определения. – М.: Стандартинформ, 2006.
3. Соломанидин Г.Г. Предложение услуг безопасности // Междунар .науч. конф. «Информатизация правоохранительных систем». Сб. тр. – М., 2001. – С. 87–89.
4. Волхонский В.В. Системы охранной сигнализации. – 2-е изд., доп. и перераб. – СПб: Экополис и культура. – 2005. – 204 с.

Волхонский Владимир Владимирович – ЗАО «Хоневелл», кандидат технических наук, доцент, руководитель направления систем безопасности, volkhonski@mail.ru