Вопросы интеграции технических средств безопасности

С.И. Козьминых,
кандидат технических наук, начальник НИЦ "Охрана"
ГУВО МВД России;
А.К. Крахмалев,
кандидат технических наук, начальник отдела НИЦ "Охрана"
ГУВО МВД России

В статье рассмотрены области применения, назначение, состав и критерии выбора интегрированных систем безопасности – нового перспективного направления развития технических средств обеспечения безопасности

В целях повышения уровня безопасности в настоящее время широко внедряются в практику интегрированные системы безопасности (ИСБ). В большинстве случаев ИСБ рассматриваются как набор технических подсистем, обладающих конструктивной, информационной, программной и эксплуатационной совместимостью и предназначенных для решения вопросов обеспечения безопасности крупных и средних объектов (банки, предприятия, учреждения, офисы и т.д.). Интегрированные системы безопасности являются наиболее перспективными средствами обеспечения комплексной безопасности объектов.

В состав технических средств ИСБ входят охранная и пожарная сигнализация (ОПС), телевизионные системы видеоконтроля (ТСВ), системы контроля доступа (СКД), а также ряд дополнитель-

Краткие характеристики системы "Рубеж-07-3":

- *информационная емкость (количество подключаемых охранных и пожарных шлейфов) – 255;*
- *количество устройств контроля доступа – 32 (64 точки доступа);*
- *количество релейных выходов для управления внешними устройствами – 160 (с возможностью расширения до 255);*
- *выход для подключения к ЭВМ, принтеру;*
- *возможность объединения по сети 255 контроллеров в систему, содержащую 65 025 шлейфов, 8160 устройств контроля доступа, 16 320 считывателей (клавиатур).*

Более подробно с характеристиками этих систем можно познакомиться в предыдущих публикациях журнала

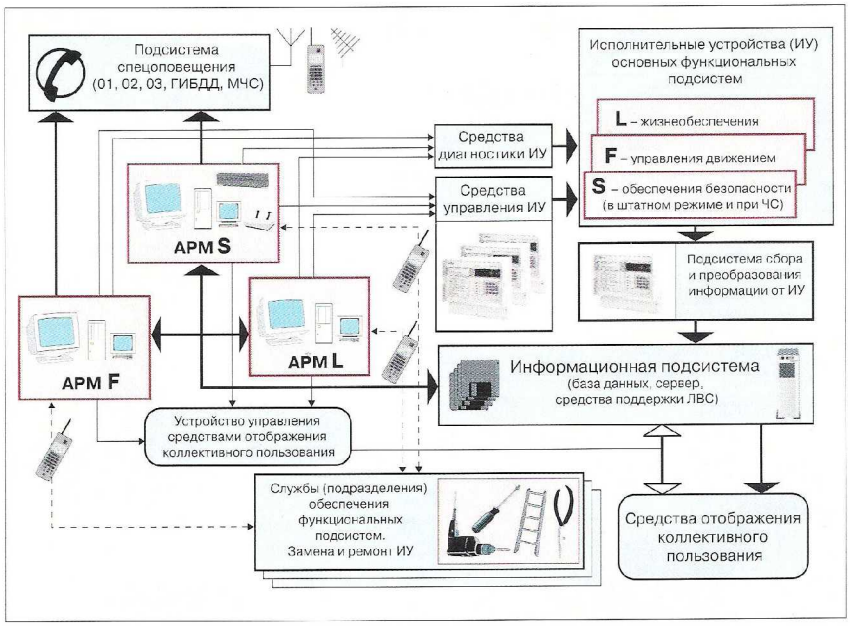

Рис. 1. Комплекс систем автоматизированного управления функционированием, жизнеобеспечением и безопасностью объекта на основе системы "Рубеж-07-3"

ных подсистем, обеспечивающих защиту от различных видов угроз, возникающих на объектах. Основная задача ИСБ – обеспечение на качественно новом уровне комплексной безопасности больших, средних и особо важных объектов, особенно кредитно-финансовых.

Примеры ИБС

В соответствии с необходимостью реализации комплексной безопасности объектов ГУВО МВД России было принято решение о включении в "Перечень технических средств вневедомственной охраны, разрешенных к применению" двух ИСБ отечественного производства, выпускаемых серийно, имеющих сертификаты соответствия ЦСА ОПС ГУВО МВД России и органа по сертификации ГУГПС МВД России, прошедших подконтрольную эксплуатацию на объектах и экспертизу в НИЦ "Охрана" ГУВО МВД России.

1. ИСБ "Рубеж-07-3" (НПФ "СИГМА – Интегрированные системы", г. Москва) предназначена для обеспечения безопасности средних и больших объектов. Реализует аппаратно-программное объединение подсистем охранной, пожарной сигнализации, контроля и управления доступом, системы телевизионного наблюдения. Имеет адресно-радиальную структуру построения. Обеспечивает такие возможности, как работа и программирование без компьютера, объединение в локальную сеть с управлением от ЭВМ и наращивание разветвленной структуры. Модульность архитектуры системы и возможности программирования на этапе подготовки проекта позволяют строить сложные программно-технические комплексы, объединяющие ИСБ с системами жизнеобеспечения объекта и автоматизированными системами управления технологическими процессами. На рис. 1 приведен пример обеспечения безопасности автомагистрального тоннеля на основе автоматизированной системы функционирования, жизнеобеспечения и безопасности "Рубеж-07-3".

Использование ИСБ позволяет обеспечить безопасность как одного учреждения, так и группы объектов, осуществляя при этом контроль, автоматизированную регистрацию всех событий и централизованное конфигурирование всей системы. Внедрение таких систем требует значительных финансовых затрат, но они меньше, чем в том случае, когда каждая из подсистем используется в автономном режиме, а эффективность применения ИСБ значительно выше.

Еще одним компонентом ИСБ, который обязательно присутствует в составе любой из подсистем, является система оповещения в виде световых и звуковых оповещателей, световых табло, мониторов компьютеров и т.д. Однако в ряде случаев **система оповещения** может представлять собой отдельную техническую систему (например, речевого оповещения, выполненную на основе радиотрансляционной сети и аппаратуры).

Кроме того, некоторые разработчики и производители ИСБ рассматривают набор технических средств, входящих в систему, более широко. Они включают в нее средства контроля и управления жизнеобеспечением объекта (электроснабжение, вентиляция, лифты, водоснабжение и др.). В этом случае ИСБ обеспечивают большие возможности и представляют собой так называемые **интегрированные системы жизнеобеспечения объекта.** Иногда применяется термин "системы интеллектуального здания".

Рассматривая ИСБ с новыми функциями, следует оценивать не только их характеристики, но и возможности для правильного выбора технических средств при планировании и проектировании общей системы безопасности объекта. В этом случае недостаточно учитывать только технические средства. Необходимо рассматривать систему безопасности в целом, т.е. как совокупность организационно-технических мер, направленных на защиту от угроз.

Существующие в настоящее время подходы к проектированию системы безопасности основаны на эвристических методах, которые рассматривают ее путем перехода от частного к общему (как совокупность компонентов, выполняющих свои задачи). При возрастании сложности систем классический (индуктивный) подход к построению оказывается малоэффективным. Создаваемая ИСБ образуется путем суммирования отдельных ее компонентов и без учета возникновения новых системных эффектов.

Для решения проблемы совершенствования ИСБ необходимы новые направления, основанные на системном подходе к анализу и синтезу, который представляет собой совокупность методов с использованием моделирования на ЭВМ.

Анализ угроз

Определение конкретных требований к безопасности базируется на анализе угроз. При этом следует рассматривать как источник угроз, так и объект защиты от них. В этих ролях могут выступать три компонента:

- человек;
- природа;
- техногенная среда (то, что создано человеком, включая и информацию).

Для подсистем охранной сигнализации, телевизионного (охранного) наблюдения, контроля доступа задачу по обеспечению безопасности можно рассматривать как организацию мер по защите жизни и здоровья людей, сохранности их собственности и экологической среды от источника угроз, возникающих в результате действий человека. Обеспечение пожарной безопасности предполагает учет взаимодействия всех трех компонентов как в качестве объектов защиты, так и источников угроз.

При планировании и проектировании системы безопасности с учетом анализа источников угроз и объектов защиты должны также подробно рассматриваться угрозы другого характера (экономические, информационные, юридические). Пример классификации угроз приведен на рис. 3.

Процесс борьбы с угрозами можно разделить на три этапа:

- предотвращение угроз (меры профилактического характера, когда угроза еще не действует, но потенциально существует. Например, для систем охраны – это техническая укрепленность объекта);
- обнаружение угроз (меры, призванные выявить угрозу в момент ее появления. Например, охранная или пожарная сигнализация);
- ликвидация последствий угроз (меры, которые принимаются после прекращения действия угрозы. Например, задержание нарушителя, тушение пожара и т.д.).

Обеспечение эффективной безопасности предполагает решение проблем моделирования угроз, их количественной и качественной оценки с учетом сложности структурно-функционального построения системы безопасности, ее элементов, а также данных о внешних воздействиях естественного и искусственного происхождения.

На прошедшей в июне 1999 года Международной конференции "Информатизация правоохранительных систем" был представлен ряд работ, посвященных вопросам комплексной безопасности объектов. Авторы статей предлагают использовать системный подход на этапе разработки концепции безопасно-

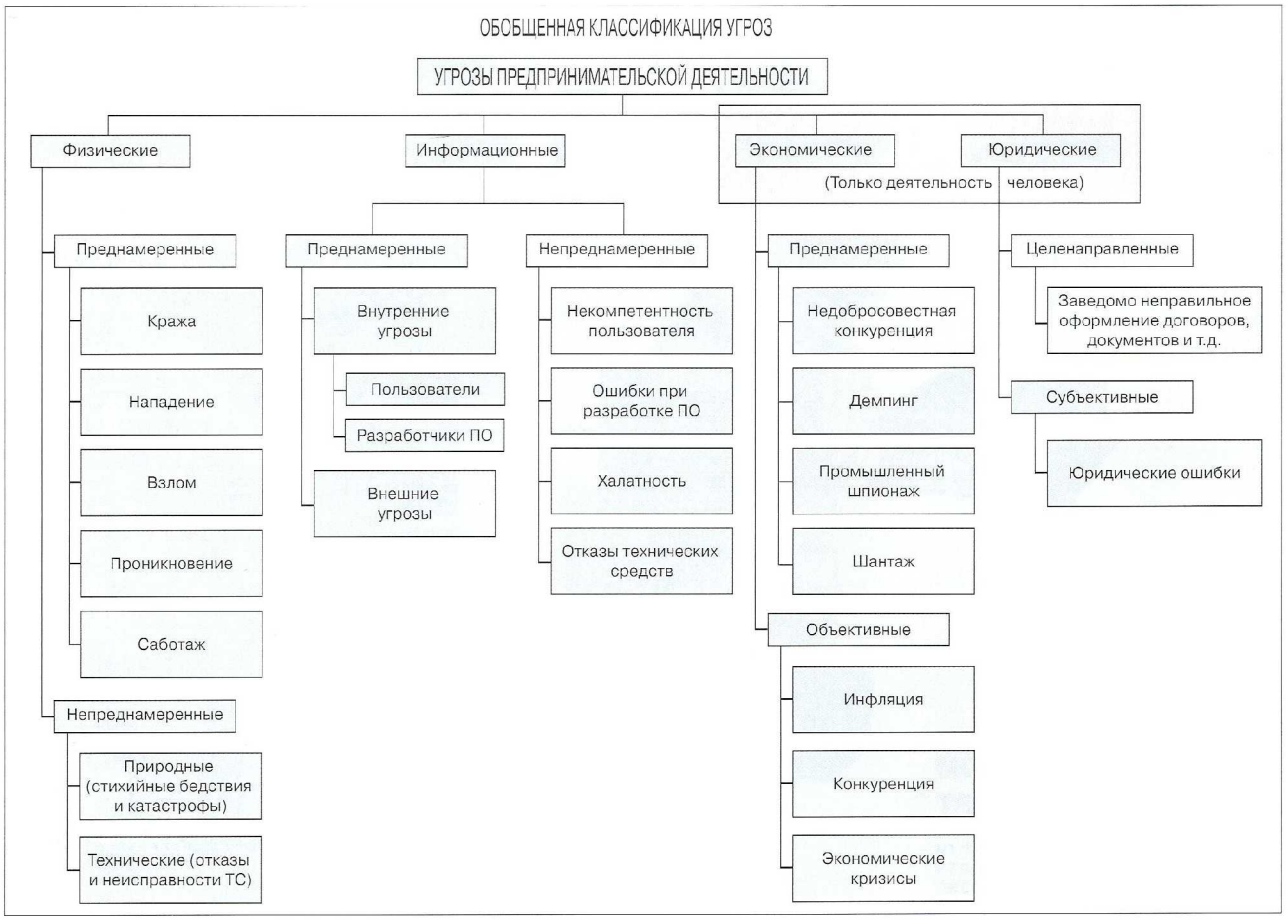

Рис. 3. Пример обобщенной классификации угроз

сти объекта, подробно рассматривают террористические угрозы, связанные с авариями и катастрофами техногенного характера, разрабатывают модели угроз для оценки степени безопасности объекта и проводят их классификацию.

Подход к классификации угроз был использован в стандарте на системы контроля доступа (СКД). Этим стандартом сформулировано понятие "несанкционированные действия" (НСД) и дана их классификация применительно к задаче контроля доступа, т.е. введен класс угроз (несанкционированные действия) и определены на описательном уровне частные модели (взлом, вскрытие и т.д.).

Для исследования моделей угроз необходимо выбрать соответствующие математические методы. При построении модели следует учитывать, что угрозы безопасности носят вероятностный характер и имеют высокую степень априорной неопределенности. При оценке угроз безопасности предлагаются:

- теория надежности для описания угроз, создаваемых техническими средствами (сбои, отказы, ошибки и т.д.);
- математическая статистика для описания естественных угроз (природные явления, стихийные бедствия и т.д.);
- теория вероятности для описания угроз, создаваемых людьми по небрежности, халатности и т.д.;
- экспертные методы для описания умышленных угроз.

В одной из работ предложен метод имитационного моделирования и разработана имитационная модель для решения задачи противопожарной защиты некоторых объектов. Достоинство такого метода в том, что исследование поведения системы проводится на ЭВМ, а не на реальном объекте. Это существенно снижает стоимость эксперимента, но должна быть доказана адекватность модели решаемой задаче.

Рассматривая основное назначение ИСБ как борьбу с угрозами различного характера, можно в качестве основного критерия для выбора систем безопасности использовать количественный показатель, связанный с числом угроз, на защиту от которых она рассчитана. Подход при определении этого критерия должен быть расширен с учетом подробного анализа угроз по укрупненным основным направлениям. Например, для подсистемы охранной сигнализации, входящей в состав ИСБ, необходимо подробное рассмотрение угроз, связанных с несанкционированным проникновением на объект.

Учитывая взаимосвязь в ИСБ организационных и технических мер обеспечения безопасности, большое значение приобретает проблема защиты информации и несанкционированного доступа к системе. Частично эта проблема была затронута при разработке стандарта на средства и системы контроля и управления доступом (ГОСТ Р 51241–98 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний").

Особое значение в современных условиях рыночной экономики приобретает необходимость обеспечения безопасности предпринимательской деятельности организаций. Кроме физической защиты людей и объектов, которая осуществляется техническими средствами ИСБ, необходимо обеспечивать экономическую, информационную и юридическую безопасность личности, собственности, предпринимательской деятельности. Для решения этой задачи в ИСБ должен быть включен дополнительный модуль, который может быть реализован программными средствами. Одним из авторов данной статьи уже была рассмотрена концепция 4 уровней сетевого взаимодействия для технических подсистем ИСБ. Первый (высший) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети ETHERNET с протоколом обмена TCP/IP и с использованием сетевых операционных систем Widows NT или Unix. На этом уровне осуществляется связь между сервером и рабочими станциями операторов и реализация работы программного модуля, обеспечивающего поддержку безопасности экономического и юридического характера. Данный модуль может быть разработан на основе современных информационных технологий, систем баз данных, экспертных систем, баз знаний. При функционировании в единой сети и единой программной оболочке можно реализовать автоматизацию процесса принятия решений в критических ситуациях.

Классификация НСД

Несанкционированные действия (НСД) – действия, целью которых является несанкционированное проникновение через устройство преграждающее управляемое (УПУ).

Взлом – действия, направленные на несанкционированное проникновение через УПУ путем его разрушения.

Вскрытие – действия, направленные на несанкционированное проникновение через УПУ без его разрушения.

Манипулирование – действия, производимые с устройствами контроля доступа без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние заграждающего устройства. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него, а следы его не будут заметны. Манипулирование включает в себя также действия над программным обеспечением.

Наблюдение – действия, производимые с устройствами контроля и управления доступом без прямого контакта с ними, целью которых является получение действующего кода.

Копирование – действия, производимые с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.

Принуждение – насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

Саботаж (состояние саботажа по ГОСТ 50776–95) – преднамеренно созданное состояние системы, при котором происходит повреждение ее части

Подводя итоги, можно отметить следующее:

- технические средства интегрированных систем безопасности (ИСБ), наиболее широко представленные на рынке, включают в себя охранную и пожарную сигнализацию, контроль доступа, видеонаблюдение;
- дальнейшее развитие ИСБ идет по направлению интеграции с системами жизнеобеспечения объекта ("системы интеллектуального здания");
- интеграция только технических средств недостаточна для решения вопросов комплексной безопасности объекта. Необходим более широкий подход, учитывающий взаимодействие мер организационного и технического плана;
- появление угроз нового характера (экономических, информационных, юридических и др.) требует включения в ИСБ дополнительных средств и подсистем для защиты от данного вида угроз. При этом объектом защиты может быть не только человек и объект, но и в целом предпринимательская деятельность предприятия;
- одним из комплексных критериев оценки эффективности ИСБ может служить количественный показатель, связанный с числом угроз, защиту от которых может обеспечить данная ИСБ.

Реализация подхода к проектированию ИСБ, предложенного в данной статье, по мнению авторов, позволит решить на качественно новом уровне проблему комплексного обеспечения безопасности предпринимательской деятельности и оптимизировать затраты, направленные на решение этих задач. ■

январь-февраль 2000