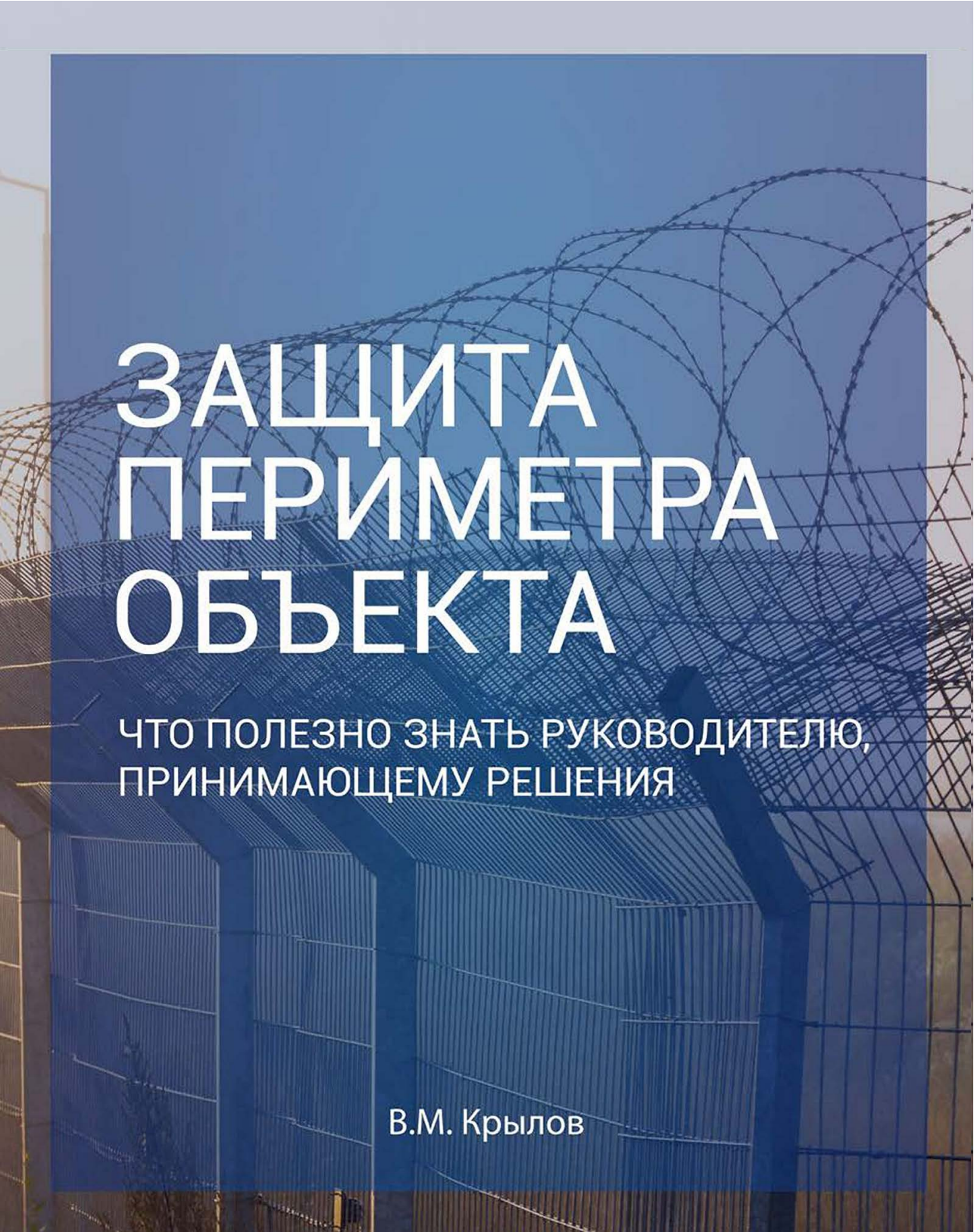


ЗАЩИТА ПЕРИМЕТРА ОБЪЕКТА

ЧТО ПОЛЕЗНО ЗНАТЬ РУКОВОДИТЕЛЮ, ПРИНИМАЮЩЕМУ РЕШЕНИЯ

В.М. Крылов

Эта книга для тех руководителей, которых мало впечатляют мигающие лампочки и красиво светящиеся экраны. Для тех, кому нужна реальная и хорошо работающая система защиты объекта и обоснованные затраты на ее создание.

Содержание

Когда системы безопасности станут оружием защиты (вместо предисловия) **4**
1. Почему СПС главная в системе безопасности **8**
1.1 Для кого эта книга 8
1.2. Правовые аспекты проблемы 10
1.3. Основные задачи комплексной системы безопасности 13
2. Что влияет на выбор СПС **18**
2.1. Какую систему выбираем 18
2.2. Где устанавливаем систему 21
2.3. Правильно ли сигнализирует СПС 24
2.4. Повышение эффективности системы за счет дополнительных рубежей защиты 31
3. Интеграция СПС с другими ТСО **33**
3.1. Две методики ТВ-наблюдения 33
3.2. Интеграция с другими с охранными системами 37
4. Как убедиться, что система работает **40**
4.1. Необходимость проведения приемо-сдаточных испытаний 40
4.2. Оценка вероятностей ошибок 41
4.3. Методы проведения приемо-сдаточных испытаний по оценке характеристик системы 46
5. Стоимость СПС **51**
5.1. Структура стоимости СПС 51
5.2. Стоимость создания СПС 52
5.3. Оценка стоимости владения 55
6. Как обучить персонал и не дать ему «угробить» систему **57**
7. Центр компетенции по системам периметральной сигнализации **60**
7.1. Задачи Центра компетенции по системам периметральной сигнализации 60
7.2. Моделирование как надежное средство оценки эффективности систем безопасности 62

Когда системы безопасности станут оружием защиты (вместо предисловия)

Немного теории

Сначала ответим на вопрос: что такое эффективное оружие? Это такое безотказное оружие, которое с высокой вероятностью поражает цель. Основными тактико-техническими характеристиками (ТТХ) любого оружия, включая системы периметральной сигнализации и комплексные системы безопасности (СПС и КСБ соответственно), в целом являются:

- вероятность поражения неприятеля – в нашем случае это вероятность обнаружения нарушителя – $\mathbf{P}_{\text{обнаруж}}$ для СПС и вероятность его задержания для КСБ – $\mathbf{P}_{\text{задерж.}}$
- вероятность ложной тревоги $\mathbf{P}_{\text{ложн}}$ (чаще используется производная величина – среднее время наработки на ложное срабатывание – $\mathbf{T}_{\text{ложн}}$).

Именно эти параметры определяют эффективность оружия, называемого системой безопасности. Конечно, важны и стоимость системы и наличие сертификатов и возможность дистанционного управления и т.п.

Этапы создания системы безопасности такие же, как при создании оружия. Чтобы оружие (КСБ, СПС) стало эффективным, его необходимо (рис. 1):

1. правильно спроектировать, выполнив требования заказчика по основным ТТХ. На что должен обратить внимание заказчик при составлении технического задания мы поговорим далее в разделах 1-3;

2. правильно и надежно построить в соответствии с проектом;

3. провести испытания (контрольные стрельбы). На основании этих испытаний делается вывод о соответствии ТТХ системы (т. е. $\mathbf{P}_{\text{обнаруж}}$, $\mathbf{T}_{\text{ложн}}$) заявленным в ТЗ требованиям. В случае их соответствия и только

после этого дается заключение о возможности применения соответствующего оружия – о выполнении КСБ, СПС своих основных функций. Какие методики используются для проведения испытаний – в разделе 4.

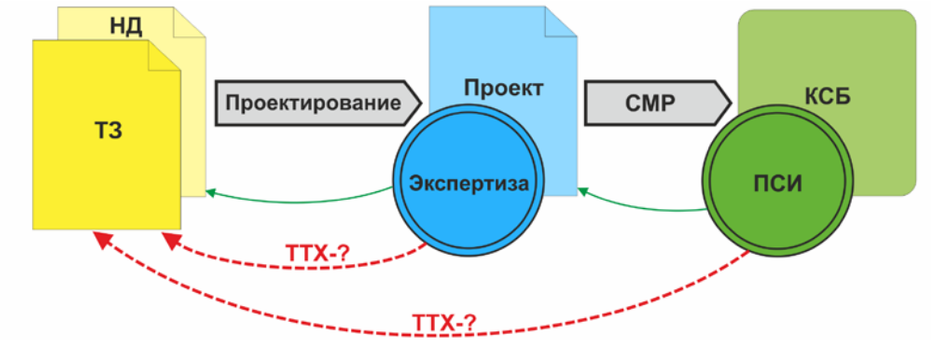


Рис.1 *Этапы создания системы безопасности*

Что на практике

К сожалению, эти вполне очевидные требования выполняются сегодня при создании СПС и КСБ лишь в малой части. Практика создания систем безопасности сегодня, увы, иная.

Требования технического задания (ТЗ) на создание СПС и КСБ формируются заказчиком и экспертами на основе оценки уязвимости объекта. Вопрос, почему на практике для абсолютного большинства объектов требуется, чтобы $\mathbf{P}_{\text{обнаруж}}$ было 0,95–0,98 (т. е. допускается проникновение каждого 20–50-го террориста), не имеет ответа. Его можно было бы задать тем, кто придумал это требование, но ответа, скорее всего мы не получим: просто так уже сложилось.

1. Проектирование. Что должен сделать проектировщик, чтобы выполнить заданные требования? Ответ кажется очевидным: использовать сертифицированные средства обнаружения. К сожалению, этого недостаточно. Во-первых, не все технические средства в принципе могут быть сертифицированы, поскольку создаются непосредственно на объекте. Это, например, относится к вибрационной периметральной сигнализации, установленной на 80-90% объектов (подробнее в главе 2 и, конкретно, в разделе 2.3).

Во-вторых, $\mathbf{P}_{\text{задерж}}$ зависит не только от технических средств (ТС) и правильного срабатывания периметральной сигнализации, но и от действий людей (охранников, операторов), их размещения, тактики действий и т.д. и т.п. Для учета этих и других, влияющих на исход, обстоятельств проектировщик сегодня располагает следующими возможностями:

- довериться мнению эксперта (своему опыту). С иллюстрации работы таких «экспертов» начинается поэма Н.В. Гоголя «Мертвые души»: «…доедет карета до Москвы али не доедет?»
- построить систему и провести ее испытание. Этим способом можно получить объективную картину. Однако, во-первых, оценить результат получится только ПОТОМ, а надо ДО – до того, как начали проектировать и строить. Во-вторых, объем, время и стоимость подобных испытаний будут велики, а чаще – неподъемны. По этим причинам при экспертизе готового проекта КСБ на практике устанавливается лишь соответствие проекта требованиям ТЗ и нормативной документации. И только это!

Поэтому и возникает **проблема №1**: оценить соответствие ТТХ проекта требованиям ТЗ до начала строительства.

2. Строительно-монтажные работы (СМР). Если работает профессиональная компания, соблюдающая действующие строительные нормы и правила, то построенная система безопасности будет соответствовать проекту. Найти такого подрядчика не проблема, это вопрос правильной организации конкурса. Заканчиваются СМР проведением приемо-сдаточных испытаний (ПСИ), чтобы проверить функционирование системы. Однако эти испытания ни в коей мере не дают информацию о том, какие ТТХ имеет построенная система безопасности. Необходимы статистические ПСИ.

3. Статистические ПСИ. Их задача оценить ТТХ построенной системы: $\mathbf{P}_{\text{задерж}}$ и/или $\mathbf{P}_{\text{обнаруж}}$ и $\mathbf{T}_{\text{ложн.}}$ Их реализация – это **проблема №2**: большой объем испытаний и отсутствие эффективных методик, но главное – отсутствие нормативного требования, обязывающего проводить подобные испытания. В результате заказчик не знает, насколько полно система выполняет свои основные функции и поэтому система

безопасности не становится оружием.

Решение проблем

Проблема №1 решается путем создания системы моделирования систем безопасности, в которой на базе имитационных моделей технических средств, поведения нарушителя, тактик службы охраны, работы операторов и др. проводятся вычислительные эксперименты. Набирается статистика по проникновению нарушителя на охраняемый объект и организации противодействия ему. При этом учитываются все особенности охраняемого объекта, варианты тактик работы охраны, ее размещение на объекте и проч. В результате полученных данных достоверно оцениваются ТТХ и осуществляется объективный и количественно обоснованный выбор решений защиты объекта. Решений необходимых и достаточных, то есть не требующих избыточных затрат.

Именно такой Автоматизированный Комплекс Имитационного Моделирования (АКИМ) разработан компанией «ПЕНТАКОН» и о нем подробнее мы остановимся в одной из глав этой книги.

Для решения **Проблемы №2** необходимы:

1. Законодательные действия, вводящие нормативные требования проводить статистические ПСИ КСБ и СПС.

2. Эффективные, уменьшающие трудозатраты методики статистических испытаний. Такие методики контрольных испытаний периметральных систем (КИПС) предлагает компания «ПЕНТАКОН». Методики КИПС построены на базе действующих ГОСТ R 27.403-2009, ГОСТ 27.402-95 и позволяют сократить на порядки объемы испытаний по сравнению с методиками доверительных интервалов. Для удобства и простоты использования методики предлагаются пользователям в виде диалоговой программы. Подробнее об испытаниях систем безопасности вообще и об эффективности методики КИПС мы расскажем в разделе 4.3.

Как театр начинается с вешалки, так и защита любого объекта начинается с защиты его периметра
В.М. Крылов

1
Почему СПС главная в системе безопасности

1.1 Для кого эта книга

В последние десятилетия обеспечению безопасности объектов и инфраструктуры уделяется все больше внимания. В тоже время существует ряд факторов, которые существенно влияют на принимаемые решения. Одним из таких факторов является изменение характера угроз, вызванное активизацией диверсионно-террористической деятельности. Рост числа проявлений терроризма привел к изменениям мер, в том числе превентивного характера, со стороны правительства, правоохранительных органов и различных организаций. Поэтому особое внимание стало уделяться безопасности объектов топливно-энергетического комплекса, атомной энергетики и транспортной инфраструктуры.

Все указанные объекты имеют одну существенную особенность – протяженный периметр, который, чаще всего, становится самым уязвимым местом. Забор, колючая проволока или другие сдерживающие заграждения уже не пугают даже самых неискушенных нарушителей, а патрулирование периметра силами вооруженных подразделений является слишком дорогим удовольствием.

Выход в данном случае есть: оснащение периметра автоматизированным комплексом технических средств, который включает систему периметральной сигнализации (СПС), телевизионное и/или телевизионное наблюдение, охранное освещение, контроль доступа и др., в совокупности обеспечивающих своевременное, достоверное и полное информирование службы охраны о происшествии. При этом главной и системообразующей в этом комплексе является СПС, так как именно от этой системы зависит своевременная передача сигнала о нарушении периметра объекта. Такие системы сложны в проектировании и установке, и требуют значительного первоначального вложения средств.

Цель данного материала вооружить руководителей компаний и собственников бизнеса набором обоснованных подходов к выбору системы обеспечения безопасности.

Руководитель находится в непростом положении: ему надо принять решение о выделении значительной суммы (1—100 млн руб. и более) на создание СПС и при этом ему нужно быть уверенным, что деньги не будут потрачены впустую. Поэтому, утверждая бюджет создания СПС, руководитель пытается ответить на следующие вопросы:

- А так ли это необходимо?
- Что произойдет, если не поставить систему? А если поставить-будет ли она эффективно работать?
- Почему мы должны поставить именно эту систему?
- А не много ли запросили соответствующие службы? Или наоборот – достаточно ли?

Эта книга поможет руководителям разговаривать с потенциальными проектировщиками и инсталляторами систем периметральной сигнализации на одном языке.

Мы хотим помочь руководителю получить ответы на эти вопросы и самостоятельно сориентироваться в некоторых непростых технических аспектах построения СПС, от правильного понимания которых зависит и эффективность работы системы и ее цена.

Также эти знания позволят квалифицированно разговаривать с потенциальными исполнителями, каждый из которых пытается убедить заказчика в том, что его система, его предложение и цена самые лучшие.

1.2. Правовые аспекты проблемы

Современная нормативно-правовая база в сфере безопасности начала формироваться еще в 90-х годах прошлого века, но и сегодня она постоянно претерпевает изменения в зависимости от возникающих угроз. Однако, как показывает практика, требования законодательных актов сводятся на нет недобросовестностью их исполнения.

Вот уже более двенадцати лет действует закон № 35-ФЗ «О противодействии терроризму» от 6 марта 2006 г., а также ряд нормативно-правовых актов Президента и Правительства Российской Федерации и регламентирующих отраслевых документов, а обеспечение безопасности жизненно важных объектов все еще далеко от совершенства. Примером тому может служить террористический акт в аэропорту Домодедово 24 января 2011 г.

Если предположить, что террористы – нарушители подготовленные, то что можно сказать о следующих случаях проникновения людей на территорию аэропорта (охраняемого объекта):

- 22.08.2013, Иркутск - «…чтобы вблизи посмотреть на самолёты…»;
- 02.12.2013, Чебоксары - «… увидеть восход солнца…»;
- 04.05.2014, Богучаны – «… чтобы сократить путь…».

Можно сказать только одно: система защиты периметра на данных объектах просто отсутствует или была сделана, как показано на рис. 2. А ведь данные нарушения могли быть предотвращены, если бы периметр указанных объектов был, в достаточной степени, оснащен системами инженерной защиты и была бы установлена комплексная система безопасности и СПС в частности.

К сожалению, на этапе становления и развития законодательства в сфере обеспечения транспортной безопасности (да и в сфере безопасности ТЭК тоже) большое внимание уделялось контролю доступа, системам досмотра и ТВ-наблюдению, а вот защите периметра объ-

Рис.2 *Пример оборудования аэропорта «инженерно-техническими системами»*

ектов уделялось крайне незначительное и поверхностное внимание. Это касалось как транспортных объектов вообще, так и аэропортов в частности. Поэтому и появлялись такие системы безопасности, как на уже упомянутом рисунке, причем этот аэропорт с такой уникальной системой далеко не единственный на территории нашей огромной страны.

Со временем правовые акты изменялись, все более отражая реалии времени. Так были внесены изменения в основной закон по транспортной безопасности N 16-ФЗ от 09.02.2007 «О транспортной безопасности», появились постановления, определяющие требования по обеспечению транспортной безопасности, в том числе требования к антитеррористической защищенности объектов (например, Постановление Правительства РФ от 14 сентября 2016 г. №924), были определены требования к систем обеспечения безопасности и правила их сертификации (Постановлении Правительства № 969 от 26 сентября 2016 года).

Конечно, и на современном этапе развития российского законодательства есть место для изменений, но радует то, что сегодня, в некото-

рых законодательных актах, сделаны попытки более четко определить требования к функциональным свойствам систем безопасности. Так в принятом 26 сентября 2016 года Постановлении Правительства № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности» делается попытка конкретизировать требования к СПС, а также вводится предписание проводить испытания с целью сертификации уже созданных систем. Данные положения обязывают руководителей предприятий ставить не просто какие-то системы «для галочки», а внедрять полноценные, соответствующие определенным требованиям и сертифицированные, системы безопасности, включая и СПС.

Все системы периметральной сигнализации должны быть сертифицированы на месте установки.

Невыполнение требований указанных выше законодательных актов, напрямую, не связано с возможным возбуждением уголовных дел в отношении сотрудников и топ-менеджеров предприятий: можно лишь отделаться «легким испугом» по статье 11.15.1 Кодекса РФ об административных правонарушениях. Данная статья определяет наказание для должностного лица в виде максимального штрафа в размере 100 тыс. рублей или ареста на 10 суток, а в случае привлечения к ответственности юридического лица возможно приостановление деятельности предприятия на 90 суток. А это уже дополнительные материальные потери, в том числе и упущенная выгода.

Однако если произойдет серьезное нарушение, в частности связанное с травмированием или гибелью людей, то, согласно действующему УК РФ, владельцы аэропортов, топ-менеджеры и сотрудники авиационной безопасности (САБ) могут получить реальные сроки заключения.

Например, ст. 263.1 УК РФ «Нарушение требований в области транспортной безопасности» предусматривает срок лишения свободы до 8 лет. Согласно положениям этой статьи если с любителями «…вблизи посмотреть на самолёты…» что-то произойдет или их действия повлекут серьезные последствия, то отвечать за это будут не только любители (по другой статье и вероятно по КоАП РФ), но и, в первую

очередь, руководитель и сотрудники САБ.

Другая статья УК РФ ст. 238 «Производство, хранение, перевозка либо сбыт товаров и продукции, выполнение работ или оказание услуг, не отвечающих требованиям безопасности» предусматривает лишение свободы на срок до десяти лет. В случае серьезного происшествия эта статья может быть применима уже к руководителям предприятия.

До 10-ти лет лишения свободы могут получить руководители предприятия.

К сожалению, управляющие компании приватизированных аэропортов не спешат выделять деньги на оснащение периметра техническими средствами охраны, в других — ждут выделения денег от государства в лице Росавиации. В общем, пока гром не грянет, мужик не перекрестится. Впрочем, «грома» ждут не только на предприятиях транспортной сферы, но и на других объектах критической инфраструктуры.

1.3. Основные задачи комплексной системы безопасности

Как уже отмечалось, сегодня особенно остро стоит проблема защиты, например, таких объектов как нефтехранилища, аэропорты, склады готовой продукции, большие автостоянки, и т.п., прежде всего, из-за протяженности охраняемого периметра. В ряде случаев такие объекты имеют внутри периметра другие защищаемые зоны, что еще более усложняет задачу.

Защитить такие объекты силами только службы охраны просто невозможно. Даже в древние времена для защиты периметров использовались различного рода инженерные сооружения - крепостная стена, ров с водой, а для сигнализации – веревочка с колокольчиками. И если применяемые для защиты периметра средства с течением времени видоизменялись, вбирая в себя новые достижения инженерной мысли (хотя суть многих из них - забор, решетка - сохранилась), то человек остался таким же, как и несколько веков назад.

Речь идет, прежде всего, о психофизиологических способностях человека. Например, время реакции на события у среднего индивидуума составляет от 0.3с до 1.5с. При этом он способен удержать внимание не более чем на 10 предметах. Если же говорить о сотрудниках служб безопасности, которым приходится круглосуточно и непрерывно анализировать одни и те же изображения с телевизионных камер наблюдения, то в данном случае на первый план выходит усталость как общефизическая, так и зрительная, когда происходит так называемое «замыливание» и пропуск изменений картинки (соответственно пропуск нарушителя). Кроме того, охранники просто могут быть или добросовестными или нерадивыми (рис. 3).

Во все времена безопасность объектов обеспечивают люди. Автоматизировать их труд по защите периметра и сделать его эффективным должна система периметральной сигнализации.

Поэтому все чаще на смену человеку приходят автоматизированные системы, которые не засыпают, не ищут развлечений, а лишь выполняют тот набор функций, который был заложен производителем или инсталлятором. При этом основные функции, выполняемые системой, остаются неизменными:

Задача комплексных систем безопасности не показать «крутизну» объекта, а обеспечить оперативное принятие адекватных и безошибочных решений.

- сдерживание проникновения: один или несколько рубежей ограждений и препятствий должны задержать нарушителя на время большее, чем потребуется для формирования эффективного противодействия;
- установление факта или попыток проникновения (в данном случае основную роль играют СПС);
- оценка возникшей угрозы: где, каким образом, сколько нарушителей, какое они имеют оснащение и т. п.;
- организация противодействия.

Сдерживание нарушителя обеспечивается ограждением и препятствиями, а организация противодействия на 90% зависит от действий

оперативной группы. А вот технические средства нужны, в первую очередь, для передачи сотрудникам охраны значимой информации о

Рис. 3 *Ваша система периметральной сигнализации автоматизирует труд какого охранника*

происшествии, позволяющей сделать выбор эффективных мер противодействия. При этом значимая информация должна передаваться (рис. 4):

- **своевременно**. Сигнал о нарушении должен передаваться в режиме реального времени (или близком к нему) для того, чтобы был запас времени для организации противодействия;
- **достоверно**. Система должна выдавать минимальное количество ложных сигналов о нарушении (в идеале ни одного), так как ложные срабатывания приведут к психологическому напряжению;
- **полно**. Полнота информации необходима для комплексной оценки ситуации в месте (и рядом) нарушения границы периметра и выбора эффективных мер противодействия.

Своевременность и достоверность информации обеспечивает СПС (рис. 4). Она должна обнаружить нарушителя в тот момент, когда он только начал проникновение на объект и оперативно передать информацию другим подсистемам, например, системе охранного телевидения, которая обеспечит полноту информации. При этом от достоверности сигнала СПС будут зависеть все дальнейшие действия сотрудников

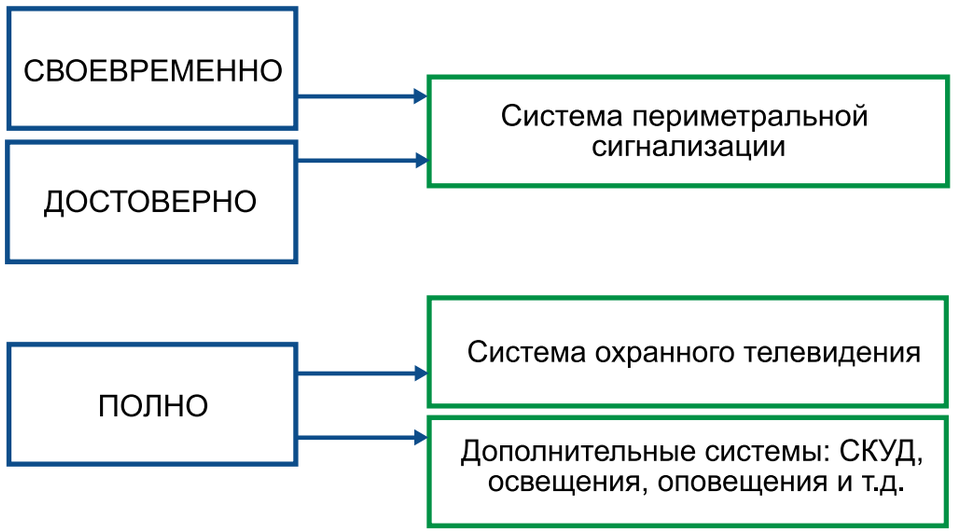


Рис. 4 *Подсистемы КСБ и их основные задачи*

службы охраны. Поэтому главной и системообразующей в инновационной комплексной системе безопасности (КСБ) должна быть СПС.

Таким образом, современные инновационные КСБ позволяют повысить эффективность труда сотрудника службы охраны и минимизировать последствия ошибок, связанных с его психоэмоциональными особенностями, путем передачи только значимой информации, которая свидетельствует о нарушении периметра объекта (тревожное сообщение от СПС, сопровождаемое информацией от системы охранного телевидения о количестве и направлении движения нарушителей) и могут снизить роль человека в процессе анализа ситуаций, обработки изображений и даже принятия решений, выдавая оператору сценарии действий. При этом от качества работы СПС будет

Система периметральной сигнализации обязана обеспечить своевременное и достоверное обнаружение нарушителя.

Система периметральной сигнализации является главной и системообразующей в современных КСБ.

полностью зависеть качество работы всей КСБ.

Далее рассмотрим основные характеристики СПС и какие параметры нужно учитывать при выборе таких систем.

2
Что влияет на выбор СПС

2.1. Какую систему выбираем

Чтобы сделать разумный выбор, надо прежде всего знать, без чего можно обойтись
Иммануил Кант

Сегодня на российском рынке существует большое разнообразие СПС как в плане их построения, так и эффективности. Как выбрать именно то, что необходимо для решения такой интересной и непростой задачи как охрана периметра конкретного объекта? Попробуем ответить на этот вопрос.

На рис. 5 показана упрощенная схема выбора варианта построения СПС.

Оптимальный вариант, чаще всего, выбирается исходя из требований заказчика, требований законодательства и бюджета. С другой стороны, характеристики объекта и модели угроз также влияют на выбор оборудования для СПС. При этом еще до начала проектирования следует провести анализ уязвимости объекта и оценку уже существующей системы безопасности. Какие методы позволяют сделать это наиболее эффективно мы расскажем в главе 7.

В настоящее время разработано огромное количество различных датчиков (основных чувствительных элементов СПС), действие которых основано на различных физических принципах, например:

- радиолучевые;
- радиоволновые;
- вибрационные (с сенсорными кабелями, сейсмические);

Рис. 5 *Схема выбора варианта построения СПС и КСБ*

- оптоволоконные;
- инфракрасные датчики (пассивные и активные);
- емкостные.

Чувствительные элементы СПС могут располагаться на ограждении, под землей, над землей (в воздушном пространстве) и на водном рубеже.

Все указанные датчики имеют свои достоинства и недостатки, а также особенности применения и монтажа. Например, для защиты открытых пространств (например, для создания выделенных зон внутри периметра), чаще всего, используются радиолучевые датчики, принцип действия которых основан на выявлении приемником изменений электромагнитного поля, созданного передатчиком под воздействием объекта - нарушителя. К сожалению, использование таких систем имеет рад ограничений: они могут использоваться только на участках

Более 80% российского и мирового рынка СПС занимают вибрационные системы обнаружения.

прямой видимости. С другой стороны, емкостные датчики, реагирующие на касание к ограде за счет изменения электрической емкости, дают большое количество ложных срабатываний в условиях близкого расположения источников электромагнитного поля.

В настоящее время наибольшее распространение получили вибрационные системы, которые занимают более 80% российского рынка. Они подходят к любому рельефу и различной конфигурации ограждения, и отличаются хорошей помехозащищенностью. Большинство из представленных на рынке – это трибоэлектрические системы. Однако сегодня набирают популярность системы на основе проводной радиолокации, которые, по сравнению с трибоэлектрическими системами, имеют ряд преимуществ, о которых будет сказано далее.

К сожалению, стоит отметить, что большинство СПС устанавливаются на объекте только потому, что так требует закон. Но такой формальный подход сказывается на работоспособности системы, так как после установки на объекте и введении в эксплуатацию уже никто не проверяет сигнализирует ли система и правильно ли она это делает. Это происходит потому, что производитель оборудования указал, что система обнаруживает нарушителей на все 100% и инсталлятор и, самое главное, заказчик ему поверили. По сути же может оказаться, что система есть, есть ощущение, что она работает, но нарушители спокойно пересекают периметр. Почему же так происходит?

Многие введенные в эксплуатацию СПС не выполняют свою главную функцию - достоверно сигнализировать о нарушении периметра.

Происходит это потому, что в техническом задании (ТЗ), чаще всего, указывается, что СПС должна обеспечить обнаружение нарушителя с вероятностью не менее 95%. Такие же показатели (или выше) указывают производители оборудования. Другими словами такая система может спокойно пропустить каждого 20-го нарушителя. Однако данные, которые указал производитель, соответствуют лишь определенным условиям и на реальном объекте могут сильно отличаться от заявленных. Почему так происходит объясним в следующих разделах.

2.2. Где устанавливаем систему

Все объекты индивидуальны и имеют свои особенности. Поэтому при проектировании СПС следует учитывать множество факторов, таких как:

- месторасположение охраняемого объекта;
- характер и тип инженерного заграждения;
- наличие вблизи зон обнаружения линий электропередачи и растительности;
- характер рельефа местности и т.д.

В зависимости от перечисленных факторов следует выбирать, где и как будет располагаться СПС:

- на ограждении;
- под землей (сейсмические);
- в воздушном пространстве (не на ограждении).

Чаще всего СПС монтируют на уже имеющемся ограждении. Это могут быть бетонные заборы, цельнометаллические, сварные конструкции или просто колючая проволока. В зависимости от типа ограждения на них монтируют различные типы чувствительных элементов СПС, чаще всего, виброчувствительные кабели.

Как уже говорилось, вибрационные системы занимают более 80% российского рынка. Причем из этой доли рынка большую часть занимают трибоэлектрические системы, чаще всего в силу «традиций» и более низкой стоимости базового элемента (хотя в совокупности общая стоимость СПС на протяженных объектах может быть значительно выше, чем у альтернативных систем. Но об этом расскажем в следующих разделах). Однако сегодня трибоэлекстрические системы начинают теснить системы на основе проводной радиолокации, которые, по сравнению с трибоэлектрическими системами, имеют ряд преимуществ, в

том числе в плане настройки чувствительности системы и снижения количества ложных срабатываний.

Для установки вибрационных систем годится любое вибрирующее под действием нарушителя ограждение: цельнометаллическая сетка, сетка «Рабица», профлист и т. п. В случае жестких (бетонных) заборов, сверху надо установить армированную колючую ленту (АКЛ) типа «Егоза» (хуже проволочный козырек), на которой закрепить сенсорный кабель (рис. 6а). Некоторые производители, иногда, утверждают, что система будет работать, если проложить кабель как показано на (рис. 6б). Конечно, система сработает, но только в случае разрушения бетонного полотна, например, танком.

Практика показывает, что недопустимо часто создаются СПС, которые хорошо обнаруживают либо ворон, либо проникновение танков.

Впрочем, есть еще один маленький нюанс: при установке на АКЛ или колючую проволоку кабель должен обязательно иметь стальную защитную оболочку (броню). Например, такая броня есть у кабеля системы СТРАТУМ (см. рис. 7).

Если этим пренебречь, то уже через год-полтора система гарантированно выйдет из строя, поскольку или острые края АКЛ, или основа ленты повредят пластиковую оболочку (рис. 8) со всеми вытекающими последствиями. Кабель, в этом случае, будет являться самым слабым звеном системы и прослужит недолго.

а. *Проект* **б.** *Реализация*

Рис. 6 *Пример СПС одного из российских аэропортов*

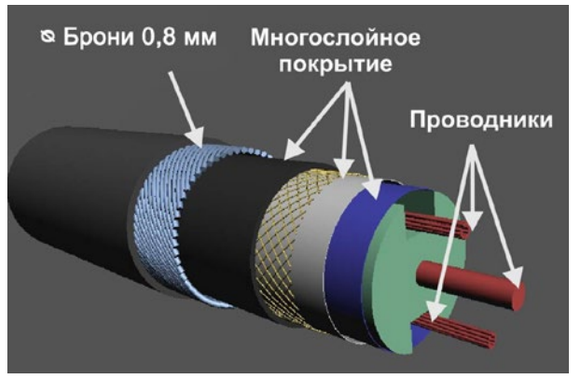


Рис. 7 *Бронированный кабель СТРАТУМ*

В настоящее время все кабельные СПС, построенные на основе трибоэлектрического эффекта, не имеют бронированной версии кабеля (это связано с особенностью трибоэлектрического принципа детектирования). Бронированный кабель используется в системах, построенных на основе проводной радиолокации. Например, СТРАТУМ.

СПС на принципе проводной радиолокации лишены многих недостатков трибоэлектрических систем.

И еще один не менее важный практический вопрос, часто возникающий у заказчика в самом начале и существенно влияющий на общую стоимость решения: какую СПС можно использовать на уже существующем заборе, часто состоящем из ограждений разного типа? Разумеется, не ухудшая при этом достоверность обнаружения нарушителя? Пра-

Рис. 8 *Повреждение оболочки виброчувствительного кабеля, смонтированного на АКЛ*

вильный ответ – только систему построенную на основе проводной радиолокации. Почему? Ответ в следующем разделе.

2.3. Правильно ли сигнализирует СПС

Обычно в рекламных материалах и технических обзорах приводятся следующие характеристики СПС:

1. **Вероятность обнаружения.**
   Под вероятностью обнаружения ($\mathbf{P}_{\text{обнаруж}}$) понимается вероятность выдачи сигнала тревоги при пересечении нарушителем зоны действия системы. Считается, что ее величина должна быть не менее 95%. Однако, как будет показано в следующих разделах, в различных условиях эксплуатации значение этого параметра может варьироваться в достаточно больших пределах и сильно отличаться от показаний, полученных в результате стендовых испытаний в лабораторных условиях.
2. **Время наработки на ложные срабатывания.**
   Время наработки на ложные срабатывания ($\mathbf{T}_{\text{ложн}}$) – среднее время наработки на ложные срабатывания. Если система часто выдает ложные сигналы о нарушении, то это может привести к потере «доверия» персонала.

Типовое ТЗ содержит требование вероятности обнаружения 95%. Понимает ли заказчик, что он соглашается с тем, что каждого 20-го нарушителя можно пропустить на объект?

Несомненно, СПС всегда должна правильно сигнализировать при нарушении периметра. Но от чего это зависит? Какие принципы должны быть использованы при построении СПС для обеспечения минимальных вероятностей ошибок обнаружения нарушения периметра? Незнание правильных ответов на эти ключевые вопросы очень часто приводит к тому, что заказчик получает систему с недопустимо большим уровнем ошибок. То есть фактически система

не будет работать, будучи полностью функционально исправной. И это случается, чаще всего, при большой протяженности охраняемого периметра.

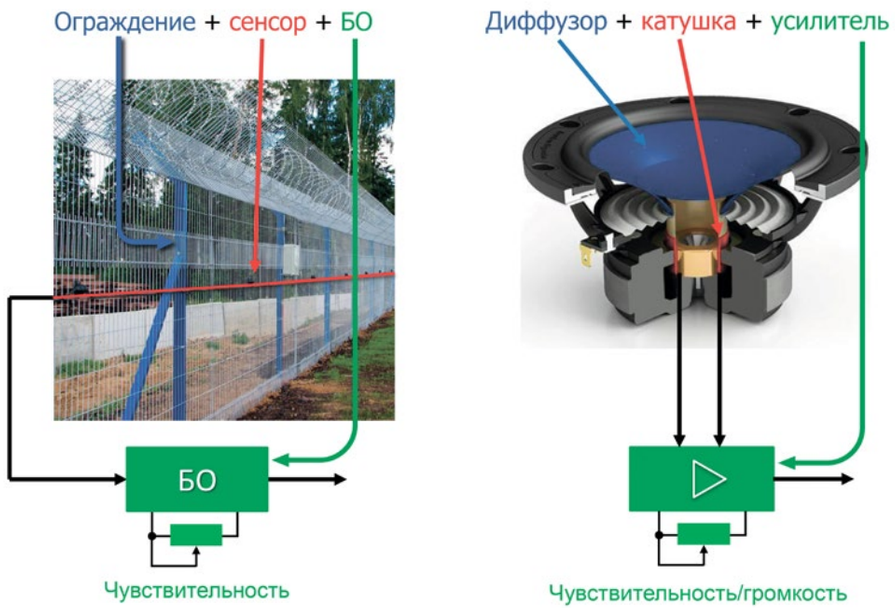
Как уже отмечалось выше, стандартное ТЗ на создание СПС требует, чтобы вероятность обнаружения составляла 95–99%. Почему считается допустимым не обнаруживать в среднем каждого 20-100-го нарушителя, неизвестно – это вопрос к тем, кто формировал это требование. При этом система должна выдавать не более 30-40 ложных срабатываний в год. Как же выбрать СПС, соответствующую указанным требованиям?

На первый взгляд ответить на этот вопрос очень просто: надо лишь заглянуть в техническую документацию оборудования. Именно так следует поступить, интересуясь характеристиками ТВ-камер, тепловизоров, досмотрового оборудования и т.д. Но в отношении характеристик СПС это абсолютно неверный ответ! Почему? Объясним это коротко, с легким погружением в школьную программу.

Если в документации на оборудование для любой вибрационной СПС указаны конкретные значения $P_{обнаружс}$ и $T_{ложн}$, то производитель этого оборудования либо недостаточно образован, либо мошенник.

Далее будет рассматриваться вибрационная система, монтируемая на ограждении (как наиболее распространенный вариант). Однако общая логика анализа и основные выводы (с небольшими оговорками) будут справедливы и для систем других типов: подземного базирования (используются, когда рубеж охраны требуется сделать невидимым), радиолучевых датчиков (например, используемых как второй рубеж охраны) и др. В перечисленных системах также не всегда можно достоверно сказать какими характеристиками будет обладать построенная СПС и совпадают ли они с заявленными производителем параметрами.

Вибрационная система обнаружения (рис. 9а) включает собственно ограждение, закрепленный на нем сенсорный кабель или вибродатчики и блоки обработки (БО) сигнала. Вибрации ограждения, вызываемые нарушителем, преобразуются сенсорами в электрический сигнал, анализируя который, БО вырабатывает (да/нет) сигнал о нарушении периметра. Этот единый, неразделяемый «виброэлектронный» ком-



а. *Вибрационная система обнаружения*

б. *Электромагнитный микрофон*

Рис. 9 *Виброэлектронные системы*

плекс «ограждение + сенсор + БО» создается на объекте усилиями двух предприятий: производящего оборудование и выполняющего инсталляцию. А заказчику и эксплуатанту системы интересны характеристики этого комплекса, которые можно оценить только после создания СПС на объекте.

Полностью аналогичен рассматриваемой системе другой «виброэлектронный» комплекс, известный нам еще со школы под названием «электромагнитный микрофон/телефон» (рис. 9б). Разве придет в голову производителю катушек индуктивности заявлять в своей документации о замечательных характеристиках и качестве звучания еще не созданного микрофона? Однако абсолютное большинство производителей электронных компонентов СПС заявляют о характеристиках еще не созданных систем. Очевидно, что подобные заявления некорректны, недостоверны и вводят покупателя в заблуждение. Их следует трактовать как недобросовестную конкуренцию. Почему? Рассмотрим далее.

На каждом конкретном объекте вероятность обнаружения зависит от конкретной инсталляции (типа ограждения, особенностей его установки, крепления кабеля и т.д.). Кроме того, необходимо определить способ и место преодоления ограждения, размеры зон охраны и общую длину периметра, погодные факторы, имеющиеся сосредоточенные воздействия и т. д. Зафиксировав весь этот набор факторов и воспользовавшись, например, методикой ГОСТ 20.57.304-76, мы за 30-300 испытаний получим оценку вероятности ошибки обнаружения именно для этих фиксированных условий. Чтобы сделать перечисленные условия случайными, потребуется на порядки (!) больший объем испытаний, что практически нереализуемо.

Если число ложных срабатываний СПС 20 в сутки(1 в час), то охранник, имея возможность регулировки чувствительности, откорректирует под себя настройку для спокойной жизни. Какова при этом окажется $P_{обнаруж}$ никто и никогда не спросит.

А что сообщают производители оборудования? Они бодро указывают в паспортных данных $\mathbf{P}_{обнаруж}$ = 0.95…0.98. Без всяких оговорок, при каких условиях эти значения получены (если они действительно были получены). А без знания исходных данных неясно, что эти цифры означают.

Совсем грустная история с параметрами, которые приводятся в технической документации для оценки вероятности ложных срабатываний $\mathbf{P}_{ложн}$. Точнее вместо $\mathbf{P}_{ложн}$ принято оценивать ее производную величину $\mathbf{T}_{ложн}$ – среднее время наработки на ложные срабатывания, которое без всяких оговорок об условиях испытаний указывается равным 1-3 мес. Тем не менее, отнесемся к данной величине с максимальным доверием и оценим смысл приведенного значения. Для этого надо ответить на один вопрос: какой длине кабеля-сенсора соответствует приведенное значение? Логично предположить, что испытывался базовый элемент с длиной плеча кабеля до 200…250 м (более часто используется зона размером 50…100 м). Тогда при длине периметра в 10 км $\mathbf{T}_{ложн}$ = 2…6 раз/день, а при длине 30 км – $\mathbf{T}_{ложн}$ = 6…20 раз/день, что вряд ли следует признать допустимым. При таких параметрах системы сотрудники службы охраны, скорее всего,

откорректируют ее работу до приемлемого для них значения частоты сигнала тревоги, что будет сделано за счет ухудшения вероятности обнаружения $\mathbf{P_{обнаруж}}$.

Как же построить систему, имеющую минимальные вероятности ошибок обнаружения? Как на этот параметр влияет протяженность периметра? Рассмотрим подробнее.

Для наглядности упростим схематичное изображение системы, представленной на рис.9а. Представим, что базовый элемент представляет собой (рис. 10) некий блок обработки (БО), к которому подсоединены два плеча виброчувствительного кабеля, длиной $\mathbf{L_{охр}}$, закрепляемого на ограждении.

На рис. 11а приведен пример того, как распределен по длине кабеля сигнал, снимаемый с плеча $\mathbf{L_{охр}}$, при одном уровне чувствительности для всей его длины. При этом на одном участке кабеля уровень сигнала может превосходить заданный порог и БО вырабатывает сигнал тревоги (в том числе из-за случайных шумов и более высокой чувствительности кабеля), а на другом проникновение не обнаруживается, несмотря на такую же (приблизительно) величину сигнала.

Первый путь решения изложенной проблемы - выровнять вибрационные свойства системы «ограждение + кабель» по длине каждого

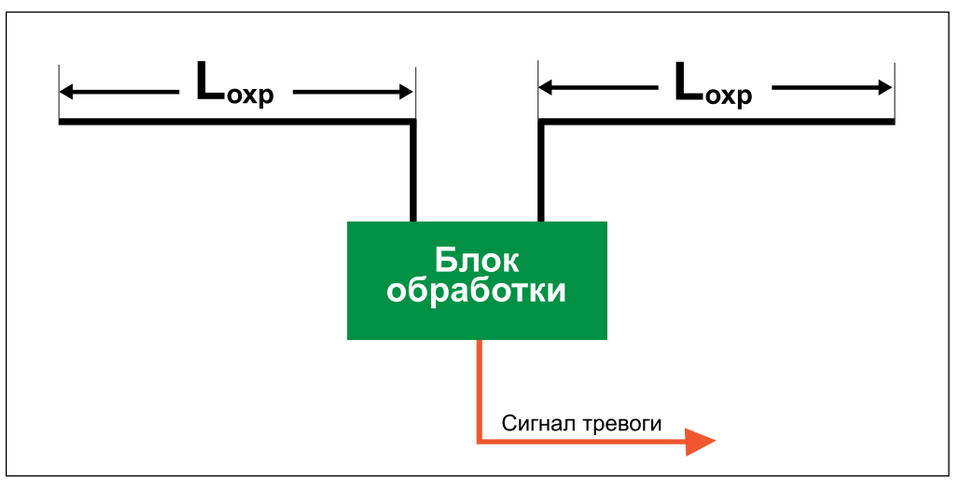
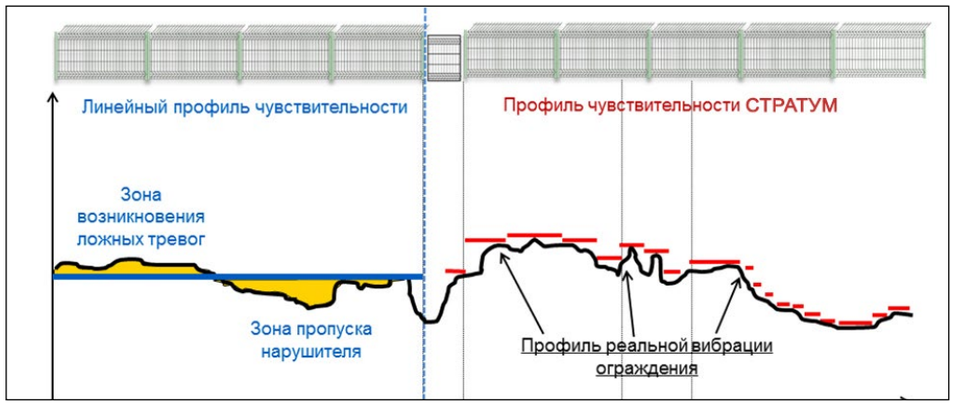


Рис. 10 *Упрощенная схема базового элемента СПС*



а ***б***

Рис. 11 *Распределение чувствительности по длине кабеля при одноуровневом и многоуровневом порогах настройки*

плеча. В практическом плане для реализации этого предложения необходимо максимально однородно (в смысле вибрационных свойств) выполнить установку ограждения и также очень качественно и однородно по всей длине осуществить крепление сенсорного кабеля. Поэтому (а не только для увеличения стоимости проекта) инсталляционные фирмы предлагают заказчику монтаж СПС вместе с установкой ограждения. Предложение заново сделать ограждение значительно повышает стоимость СПС и обычно не принимается. Тем более этим путем невозможно кардинально (в разы, а еще лучше на порядок) улучшить характеристики системы.

Кардинально улучшить характеристики СПС путем выравнивания вибрационных свойств системы «ограждение-кабель» невозможно!

Второй путь нам подсказывает рис. 11б: задавать чувствительность не одним значением на всю длину плеча (т.е. для 50…250 м) как некую «среднюю температуру по больнице», а учитывать вибрационные свойства каждой секции ограждения, т. е. с точностью 1…3 м.

В практическом плане возможны два способа осуществления этой идеи: аппаратный и программный.

В варианте аппаратного решения, например для трибоэлектрических систем, необходимо делать длину каждого плеча сенсорного кабеля величиной 1…3 м. На 200 м это все равно, что установить 200 БО, что совершенно нереально, поскольку увеличит и без того немалую стоимость СПС в несколько раз.

Программный способ задания уровня чувствительности каждого 1 м сенсорного кабеля аналогичен тому, что 200 м кабеля СТРАТУМ превращаются в 200 независимых датчиков в отличие от трибоэлектрического кабеля, в котором 200 м это один датчик (один уровень настройки чувствительности).

Программный способ задания уровня чувствительности каждого 1 м кабеля для всей 220 м длины плеча реализован только в системах проводной радиолокации (представитель таких систем – СТРАТУМ). Он не только не повышает стоимость, но и позволяет решить еще две важнейшие задачи: определить место проникновения с точностью до 1 м и минимизировать влияние интегральных воздействий (ветер, осадки, проходящий транспорт и т.п.), затрагивающих сразу несколько рядом расположенных секций.

Предлагаемый программный учет вибрационных особенностей каждого метра уже инсталлированной системы «ограждение + кабель» дает также следующие важнейшие практические преимущества:

- полностью отсутствуют требования к однородности вибрационных характеристик ограждения, которое может состоять из различных конструкций разного качества;
- при прохождении кабелем-сенсором проездов и проходов в ограждении не требуется разрезать сам кабель. Его достаточно закопать под землю и программно задать нулевую чувствительность на этих участках, т. е. задать ситуацию, когда система не будет реагировать на КАМАЗ, переезжающий кабель, но выдаст сигнал на ворону, севшую на забор в метре от дороги;
- в процессе эксплуатации системы можно (используя графический интерфейс) временно «выключить» участок периметра на период ремонтных или строительных работ.

2.4. Повышение эффективности системы за счет дополнительных рубежей защиты

Для обеспечения наилучшего результата (увеличения вероятности обнаружения $\mathbf{P}_{\text{обнаруж}}$ и снижения вероятности пропуска $\mathbf{P}_{\text{проп}}$) необходимо устанавливать не один, а 2-3 рубежа охраны.

Для обеспечения надежного обнаружения необходимо устанавливать не один, а 2-3 рубежа охраны.

Многорубежная защита (рис. 12) существенно повышает надежность охраны. Она оснащается двумя или более рубежами, расположенными на определенном расстоянии друг от друга и совмещает в себе несколько средств обеспечения безопасности. Такая система дает возможность определять направление движения нарушителя (по последовательности сигналов от СПС рубежей) и позволяет сохранить работоспособ-

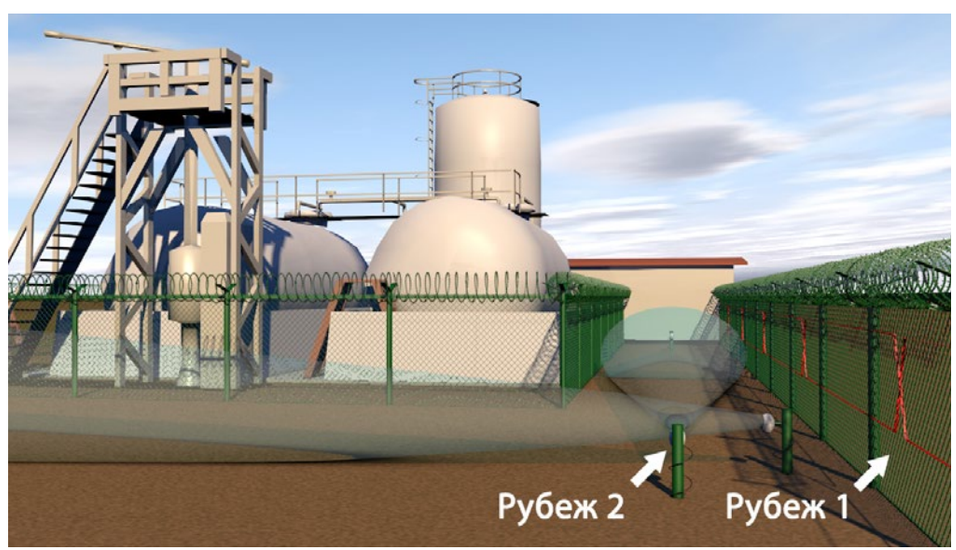


Рис. 12 *Пример многорубежной системы защиты периметра*

ность системы при выходе из строя одного из средств обнаружения. При этом на каждом из рубежей устанавливаются СПС, основанные на различных принципах обнаружения. Например, 1-й рубеж обнаружения – вибрационная система, 2-й рубеж – радиолучевые детекторы.

Что это дает? Достаточно типичное значение вероятности обнаружения $\mathbf{P}_{\text{обнаруж}}$=0.95 для широкого спектра СПС. Тогда вероятность пропуска в случае одного рубежа составит 0.05 (не обнаруживается, в среднем, каждый 20-й нарушитель), а в случае двух рубежей $\mathbf{P}_{\text{проп}}$-0.05x0.05=0.0025, т.е. пропускается лишь каждый 400-й нарушитель. Это качественно иной результат.

Два рубежа сигнализации– повышение вероятности обнаружения в 20 раз.

3
Интеграция СПС с другими ТСО

3.1. Две методики ТВ-наблюдения

Как было показано, эффективная СПС должна уметь обнаруживать факт нарушения для каждого (!) 1…3 метров длины периметра. Однако для того чтобы правильно оценить ситуацию необходимо не только узнать о нарушении периметра, но понять, что же на самом деле происходит на участке вторжения. В этом случае применяют систему ТВ-наблюдения, дополненную тепловизорами и другими системами охраны. Однако все эти устройства должны работать как единая, полноценная система - интегрированная система наблюдения за периметром.

Традиционно (назовем это Т-методикой, т.е. традиционной) весь охраняемый СПС периметр разбивается на зоны охраны, за каждой их которых наблюдают 1-2 неуправляемые ТВ-камеры. Они располагаются друг за другом вдоль ограждения на невысоких (3-5 м) столбах или прямо на ограждении (рис. 13) на расстоянии не более 50-70 м друг от друга. Указанное расстояние обусловлено разрешением стандартных ТВ-камер: если сделать расстоя-

Рис.13 *Примеры традиционного способа установки камер на расстоянии 50-70 м друг от друга*

ние больше, то оператор не сможет с необходимой полнотой и достоверностью оценить происходящее за пределами этих 50-70 м, а если поставить объектив с большим фокусным расстоянием, то он сможет разглядеть дальние рубежи, но не увидит ближайшую зону. Поэтому довольно часто выдвигаются требования об установке дополнительных камер во встречном направлении.

20 камер на 1 км – суть традиционного подхода построения комплексной системы безопасности периметра.

В этом случае каждые 100-150 м наблюдаются двумя неподвижными камерами. Это дает большее представление о том, что происходит в охраняемой зоне, но увеличивает количество необходимого оборудования, что приводит к увеличению стоимости проекта. Нередко зону охраны увеличивают (например, из-за нехватки средств) до 200-250 м, что соответствует максимально возможной длине зон охраны у большинства СПС, представленных сегодня на рынке. Однако с увеличением зон охраны резко снижается полнота и качество дистанционной оценки происходящего.

В случае нарушения периметра СПС вырабатывает сигнал тревоги, привязанный к тревожной зоне, и/или срабатывают соответствующие реле. Это дает возможность системе ТВ-наблюдения скоммутировать и вывести на мониторы наблюдения необходимые камеры, указывая

Рис. 14 *Примеры вывода изображений с камер наблюдения при их традиционной расстановке – все изображения похожи*

их номера на экране. Как это может выглядеть демонстрирует рис. 14.

Взаимодействие СПС и системы ТВ-наблюдения реализованное на уровне «сухих контактов» не может именоваться интегрированной системой.

Исходя из того, что на монитор выводятся изображения сразу с нескольких камер (рис. 14), то оперативно сориентироваться в происходящем бывает достаточно сложно, начиная с определения места расположения тревожной камеры, так как изображения со всех камер приблизительно одинаковые, а число самих камер порядка 20 шт. на 1 км. Поэтому совершенно необходимо дополнить систему охраны графическим планом охраняемого объекта с графическим же указанием зон наблюдения ТВ-камер. Кроме того, неподвижные ТВ-камеры, с узконаправленным полем зрения, установленные вдоль ограждения, не позволяют оценивать происходящее сразу же после того, как нарушитель пересек охраняемую зону. Возникает необходимость в использовании дополнительных управляемых камер и, следовательно, организации оперативного управления ими в зависимости от координат места нарушения.

Рис. 15 *Пример реализации варианта с поворотными камерами*

В силу всего сказанного такое упрощенное на уровне «сухих контактов» взаимодействие СПС и системы ТВ-наблюдения не может, с позиций современных технологических возможностей, именоваться интегрированной системой (хотя производители обычно настаивают на этом).

С другой стороны (назовем это ИС-методикой, т. е. методикой интегрированной системы) используются управляемые поворотные ТВ-камеры с трансфокатором, которые устанавливаются, как правило, на высоких 10…15 м столбах (рис. 15),

причем не обязательно расположенных возле ограждения. Это, во-первых, обеспечивает гибкость в расположении ТВ-камер и повышает эффективность наблюдения как за границей периметра, так и за частью территории объекта. Во-вторых, установка камер на высоких столбах существенно повышает их вандалозащищенность.

Например, одна такая универсальная камера стандартного разрешения с 25…30-кратной оптикой, имеющая 64 предустановки, может обеспечить качественное наблюдение за участком периметра длиной 350…450 м, т.е. потребуется не более 3-х камер на 1 км. Однако при этом необходимо оперативно управлять ТВ-камерой по 3-м координатам. При большом количестве таких камер (например, на протяженном периметре) возможно только автоматическое их позиционирование сигналами от СПС. Сама СПС в этом случае должна выдавать не просто сигнал типа «сухой контакт» о нарушении периметра в зоне 50…200 м, а указывать проникновение с точностью 3…20 м.

Расстановка ТВ-камер в соответствии с методикой интегрированной системы позволяет сократить их число в 5-7 раз и уменьшить стоимость ТВ-системы в 1.5 раза.

Все это реализовано в интегрированной системе охраны периметра СТРАТУМ.

Система СТРАТУМ работает на любом разнотипном ограждении и позволяет интегрировать охранное оборудование различных производителей.

При нарушении периметра СПС определяет координаты места проникновения и на экранах мониторов центра охраны (рис. 16) мгновенно формируются следующие изображения:

- крупным планом собственно зона нарушения (с камеры, закрепленной за этой зоной);
- общий обзорный вид примыкающей территории (с камер, расположенных по соседству);
- отображение на графическом (спутниковом) плане объекта, как места проникновения, так и графического изображения поля наблюдения камер.

Рис. 16 *Пример изображений с поворотных камер в интегрированной системе защиты периметра – на планах объекта показывается место возникновения тревоги*

3.2. Интеграция с другими с охранными системами

Люди платят нам за интеграцию, у них нет времени сутки напролет думать, что к чему подключается
Стив Джобс

СПС может интегрироваться (рис. 17) не только с системой ТВ-наблюдения (или тепловизионной), но и с системами контроля и управления доступом (СКУД), системой освещения, оповещения и т.п. Объединение различных подсистем в рамках единой КСБ позволяет решать вопросы обеспечения безопасности объекта максимально эффективно за счет того, что отдельные подсистемы как бы дополняют друг друга, взаимодействуют и обмениваются информацией. Однако эффективное взаимодействие невозможно без централизованного управления, которое позволяет составить максимально полную картину функционирования объекта и состояния его подсистем. Централизованное управление

- Система периметральной сигнализации
- Система охранного ТВ - наблюдения
- Система технологического видеонаблюдения
- Система охранно-пожарной сигнализации
- Система контроля и управления доступом
- Система тепловизионного наблюдения
- Системы передачи и хранения данных
- Системы освещения
- Системы промышленной связи(системы громкого оповещения, телефония,радиосвязь)

Рис.17 *Пример оснащения объекта системами безопасности*

также позволяет контролировать решение основных задач обеспечения защиты объекта и выполнения ряда других, например:

- автоматическое включение охранного освещения в темное время суток, например, с использованием специального управляемого прожектора;
- автоматическое позиционирование тепловизоров для оценки происходящего в условиях плохой видимости;
- автоматическое извещение всех необходимых служб;
- передача требуемой видео (и не только) информации на мобильные мониторы оперативных групп и прочие все необходимые действия;
- автоматическая организация начальных мер противодействия, например, передача нарушителю сообщений по громкой связи, дополнительное освещение места проникновения прожектором и т.п.

Все эти мероприятия являются дополнительными и хотя повышают эффективность системы защиты объекта, но не решают основные задачи: своевременно, достоверно и полно доставлять значимую информацию сотрудникам охраны. Это задачи решает только СПС, которая может взять на себя все функции централизованного управления, в совокупности с охранным телевидением. Именно они позволяют получить самую раннюю информацию о проникновении нарушителя на защищаемую территорию, на основании которой принимаются меры по нейтрализации нарушителя.

СПС может взять на себя функции централизованного управления всеми системами безопасности.

4
Как убедиться, что система работает

4.1. Необходимость проведения приемо-сдаточных испытаний

Прежде чем приступить к эксплуатации СПС, необходимо провести испытания, подтверждающие ее нормальное функционирование, соответствие всем требованиям и заявленным характеристикам. Причем это касается как вновь создаваемых, так и модернизируемых систем.

Как правило, приемо-сдаточные испытания проводятся по заранее разработанной и утвержденной программе, в которой определяется последовательность отдельных проверок и методика их проведения, а также оговаривается ожидаемый результат. Программа должна быть согласована с заказчиком и службой эксплуатации (службой охраны), разработчиком системы и монтажной организацией.

Однако не всегда приемо-сдаточные испытания (необходимость проведения которых ни в коей мере не подвергается сомнению) могут с точностью 100% сказать правильно ли работает СПС, достоверно ли формируется сигнал о нарушении периметра.

Приемо-сдаточные испытания с целью достоверной и количественной оценки обнаружительных характеристик СПС проводятся редко и неполно. Без них возможности и смысл системы периметральной сигнализации остаются неизвестными.

Известно, что достоверность – главный критерий качества работы СПС, так как цикл реагирования начинается с поступления в оперативный центр извещения о нарушении. Если поступающие извещения о проникновении нарушителя на территорию объекта недостоверны, то работа системы защиты периметра, вообще говоря, теряет всякий смысл.

Главными количественными параметрами, определяющими достоверность информации, предоставляемой СПС, являются: вероятность пропуска (необнаружения) нарушителя и вероятность ложного срабатывания. Причем эти вероятности напрямую зависят от настроек чувствительности системы.

Как уже было сказано, базовый элемент любой системы СПС (рис. 10) имеет БО, который анализирует поступающий сигнал и выдает (или нет) сигнал тревоги. При этом срабатывание БО полностью зависит от устанавливаемого в процессе пусконаладки уровня чувствительности. Следовательно, вероятности ошибок СПС зависят от результатов работы двух фирм: производителя оборудования и инсталлятора, и могут быть оценены только на уже работающей системе в ходе проведения приемо-сдаточных испытаний.

Рассмотрим, как работа системы зависит от изменения уровня чувствительности.

4.2. Оценка вероятностей ошибок

В жизни нет гарантий, существуют одни вероятности
Том Клэнси

Вероятность правильного срабатывания системы ($\mathbf{P_{прав}}$) в равной степени зависит от вероятностей двух типов ошибок: вероятности ложного срабатывания ($\mathbf{P_{ложн}}$) и вероятности пропуска цели (нарушителя) ($\mathbf{P_{проп}}$) и может быть рассчитана по формуле:

$$\mathbf{P_{прав} = 1 - P_{ложн} – P_{проп}}$$

Об этом часто забывают, требуя от разработчика и/или инсталля-

тора минимизировать только одну из ошибок – $\mathbf{P}_{ложн}$. Как правило, это возможно сделать только одновременно с увеличением $\mathbf{P}_{проп}$.

На рис. 18 показана зависимость функций распределения вероятностей $\mathbf{P}_{ложн}$ и $\mathbf{P}_{проп}$ от настройки чувствительности (порога срабатывания) системы v. Если мы выбираем настройку v2, добиваясь заданной низкой вероятности ложного срабатывания β2, мы можем получить недопустимо большую вероятность пропуска цели α2. Обратный эффект дает настройка v1. Очевидно, что с точки зрения минимизации суммарной ошибки (максимизации вероятности правильной работы системы), следует предпочесть настройку v0.

Однако здесь уместно отметить, что ошибки проявляют себя (воспринимаются сотрудниками охраны) сугубо по-разному. Большое значение вероятности ложного срабатывания $\mathbf{P}_{ложн}$=β1 (настройка v1) может привести к тому, что сотрудники охраны со временем перестанут реагировать на сигналы или попросту отключат систему. Тогда вероят-

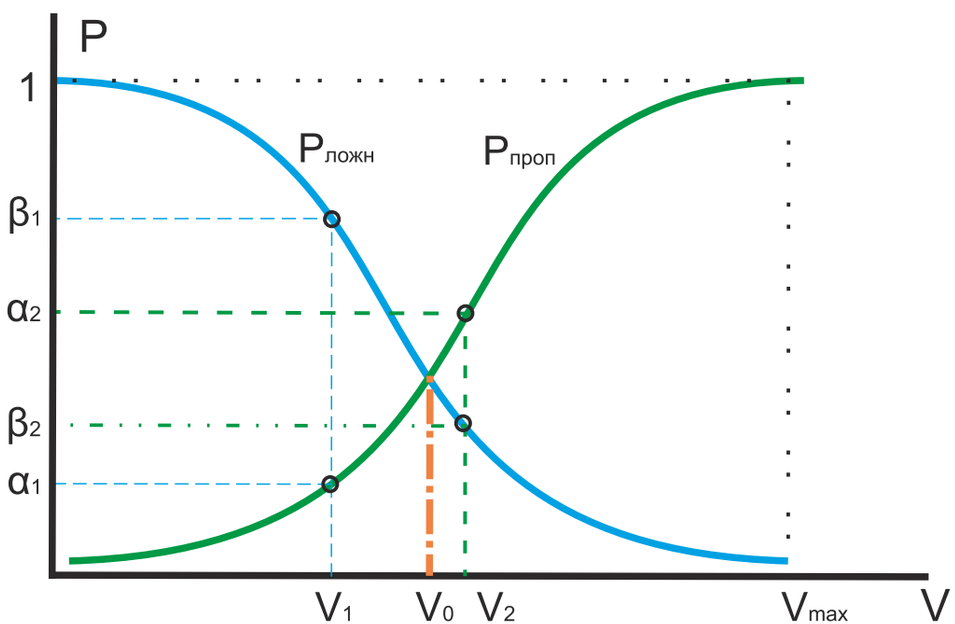


Рис.18 *Графики зависимости вероятностей ошибок от порога срабатывания (уровня настройки чувствительности)*

ность правильной работы системы становится недопустимо малой и даже близкой к нулю $\mathbf{P}_{прав} \sim 0$ ($\mathbf{P}_{прав}$=0, если систему выключат). С другой стороны возможна ситуация, когда вероятность правильной работы системы $\mathbf{P}_{прав}$ также становится недопустимо малой, но только вследствие большого значения вероятности пропуска цели $\mathbf{P}_{проп}$=α2 (настройка v2). Такая ситуация может случиться как в процессе пуско-наладки, так и в процессе эксплуатации, если инженер-пусконаладчик или охранник будут стремиться уменьшить до приемлемого (спокойного) уровня вероятность ложных срабатываний (вполне объяснимое с их стороны желание). И, что очень важно, эта ситуация сама по себе без специальных проверочных мероприятий (и, следовательно, усилий) никак себя не проявляет и не может сигнализировать о реальном положении дел. Чтобы избежать описанных ситуаций, следует настроить систему так, чтобы функции распределения ошибок $\mathbf{P}_{лож}$, $\mathbf{P}_{проп}$ не пересекались и взаимно располагались так, как это изображено на рис. 19. Тогда вероятность правильной работы системы в некоторой зоне настроек Δ будет максимально приближена к 1.

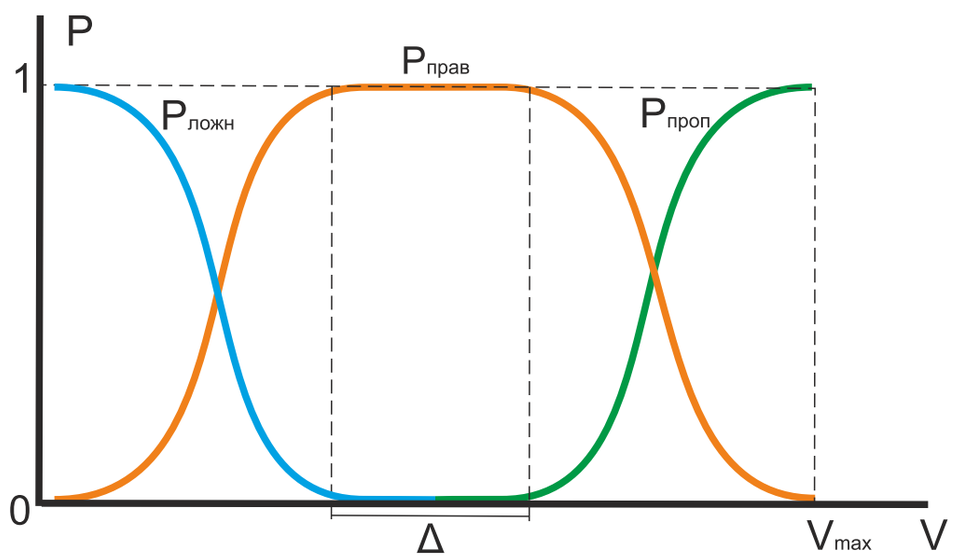


Рис. 19 *Оптимальное распределение* $\boldsymbol{P}_{ложн}$ *и* $\boldsymbol{P}_{проп}$

Укажем как изменяются относительные положения графиков распределения вероятностей для двух случаев:

- в случае более точной и детальной настройки профиля чувствительности (например, с шагом 1 м в СТРАТУМ) (рис. 20);
- в случае увеличения длины периметра (рис. 21).

На рис. 20 показано изменение расположения функций распределения вероятностей ошибок при более точной настройке профиля чувствительности (например, с шагом 1 м) на одном и том же периметре при всех прочих равных условиях. Например, на практике, настройка профиля чувствительности с шагом 1 м возможна в системе СТРАТУМ (см. рис. 11б), в то время как в трибоэлектрических системах одна зона (уровень) чувствительности составляет 50-100 м, а иногда и 200 м (см. рис. 11а). Разумеется, указанные данные не дают оснований говорить о том, что и вероятности ошибок у системы СТРАТУМ будут в 50-100 раз меньше. Но, по нашему экспертному мнению, основанному на практике множества применений, а также экспериментального сравнения систем,

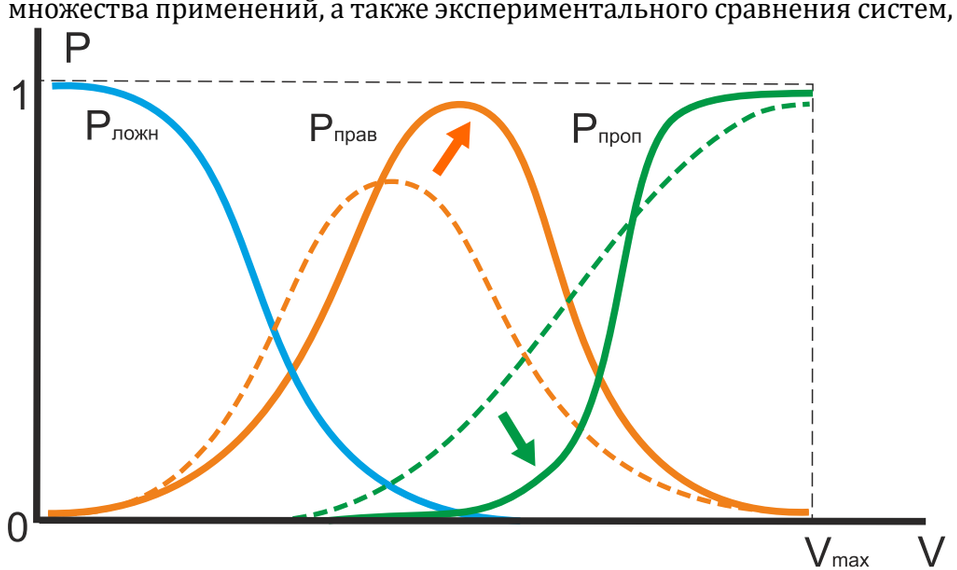


Рис. 20 *Относительные положения графиков распределения вероятностей в случае более точной и детальной настройки профиля чувствительности (например, 1 м, как в системе СТРАТУМ)*

число пропущенных нарушений периметра у системы СТРАТУМ будет, при прочих равных условиях, в 3-10 раз меньше, чем у аналогичных решений на базе трибоэлектрических систем.

На рис. 21 показано, как изменяются относительные расположения функций распределения вероятностей ошибок при увеличении длины периметра. Ввиду того, что функция распределения $\mathbf{P}_{\text{ложн}}$ смещается при этом вправо, зона настроек порога чувствительности, при которой система будет работать с приемлемым качеством обнаружения (зона, где $\mathbf{P}_{\text{прав}}$ достаточно велика), сужается. Это означает, что для любой системы существует предельная длина периметра, при превышении которой величины $\mathbf{P}_{\text{проп}}$ и/или $\mathbf{P}_{\text{ложн}}$ становятся в принципе неприемлемыми. Заметим (см. рис. 20), что в случае системы СТРАТУМ эта предельная длина будет больше (при прочих равных условиях) ввиду того, что функция распределения $\mathbf{P}_{\text{проп}}$ также смещается вправо

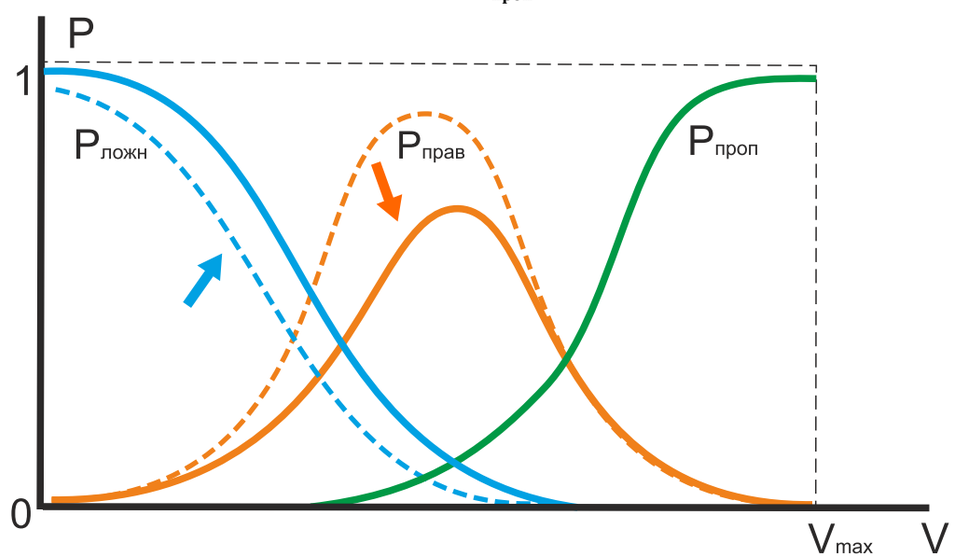


Рис. 21 *Относительные положения графиков распределения вероятностей в случае увеличения длины периметра*

4.3. Методы проведения приемо-сдаточных испытаний по оценке характеристик системы

Нас разделяют методы.., но цели у нас одни
Антуан де Сент-Экзюпери

В настоящее время приемо-сдаточные испытания проводятся в усеченном виде, так как проведение полномасштабных работ занимает значительное время, требует дополнительных затрат человеко-часов и иных средств, которые не всегда закладываются в смету или закладываются на минимальном уровне. Испытания на определение вероятности ошибок СПС не проводятся вовсе, и поэтому реальная вероятность обнаружения уже введенных в эксплуатацию систем неизвестна.

Принятое 26 сентября 2016 года Постановление Правительства № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности» предписывает проводить испытания с целью сертификации созданных СПС, однако отсутствуют утвержденные методики проведения таких работ. Где же можно взять эти методики? Рассмотрим два подхода.

Контрольные испытания– эффективная и малозатратная технология проведения приемо-сдаточных испытаний СПС с целью оценки ее обнаружительных характеристик.

Определительные методы

Для подтверждения требуемых характеристик СПС обычно рекомендуют один из двух определительных статистических методов оцен-

ки вероятности обнаружения и наработки на ложное срабатывание: точечной оценки и доверительных интервалов. Недостаток точечной оценки хорошо известен и остро проявляется при небольшом количестве экспериментов для оценивания близких к 0 или 1 параметров ввиду неприемлемо большой дисперсии оценки. Например, если из 20 проведенных экспериментов в 20 случаях нарушитель был обнаружен, то следует ли из этого, что вероятность обнаружения равна 100%? Очевидно, что нет.

Поэтому кроме точечной оценки желательно знать границы оцениваемого параметра, то есть интервал оценок, который с достаточно высокой вероятностью «накрывает» оцениваемый параметр. Обычно нормируемое значение вероятности обнаружения для СПС равно 0.95. Для подтверждения этого норматива на испытаниях, при использовании метода доверительных интервалов, потребуется проделать, например, 66 экспериментов по преодолению ограждения при условии, что в 65 из них будет зафиксировано срабатывание СПС. В этом случае можно утверждать, что с доверительной вероятностью 80% истинное значение вероятности обнаружения находится в доверительном интервале, нижней границей которого является нормативное значение 0.95. В случае же если нормируемое значение вероятности обнаружения равно 0.98, то необходимое количество экспериментов, при прочих равных условиях, будет уже 170. Т.е. этот метод подтверждения выполнения требований к СПС может оказаться весьма длительным и дорогостоящим занятием (рис. 22).

Определительные методы оценки вероятности обнаружения и наработки на ложное срабатывание СПС неэффективны и трудозатратны.

Для подтверждения другого показателя — заданной средней наработки на ложное срабатывание — суммарная наработка СПС на испытаниях должна значительно превышать нормируемое значение (как правило, это 600 часов и более). Очевидно, что метод доверительных интервалов для подтверждения таких показателей на практике неприменим.

Нормируемое значение	Число/время успешных испытаний			
	Дов.вер. = 0,8	Риск = 0,2	Дов.вер.= 0,95	Риск = 0,05
$P_{обнаруж}$ = 0,95 $P_{обнаруж}$ = 0,98	66 170	14 33	110 240	21 48
$T_{ложн}$ = 600 час $T_{ложн}$ = 1000 час	936 час 1656 час	31 час 52 час	1800 час 3024 час	134 час 233 час

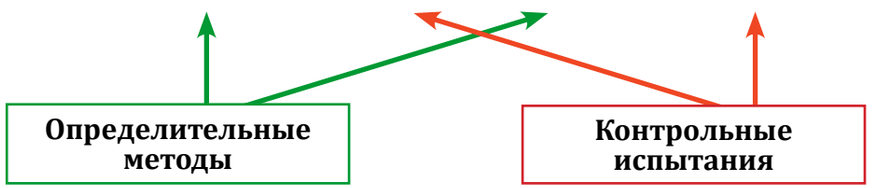


Рис.22 *Количество необходимых экспериментов и временные затраты при различных методиках проведения приемо-сдаточных испытаний*

Контрольные испытания

Корпорация «ПЕНТАКОН» предлагает новый подход к экспериментальному подтверждению показателей качества СПС. В основе разработанных компанией методик лежат апробированные, соответствующие нормативным документами и действующим ГОСТам, методы статистического контроля показателей надежности технических изделий.

В отличие от указанных выше методов точечной оценки и доверительных интервалов, применяемых с целью определения фактических показателей, мы предлагаем проведение контрольных испытаний, целью которых является подтверждение соответствия показателей качества установленным требованиям ТЗ.

Контрольные испытания позволяют снизить количество проводимых экспериментов в несколько раз.

Определительная и контрольная постановка задачи имеют суще-

ственные отличия. Постановка задачи контроля формулируется как задача проверки гипотез о том, приемлемо или нет значение показателя, которое выбирается исходя из имеющихся ограничений по длительности/стоимости испытаний. По сравнению с определительными испытаниями необходимый объем экспериментов может быть существенно сокращен при сопоставимой достоверности. Обычной мерой достоверности при проведении контроля являются равные между собой значения рисков заказчика и поставщика, соответствующие одному из значений — 0.05, 0.1 или 0.2.

Продемонстрируем возможности предлагаемого подхода на рассмотренном ранее примере. Для контроля нормативного значения вероятности обнаружения 0.95 потребуется провести 18 экспериментов по преодолению ограждения (вместо 66), из которых не менее чем в 17 должно быть зафиксировано срабатывание СПС. Тогда при рисках поставщика и заказчика, равных 0.1, принимается решение о соответствии показателя вероятности обнаружения заданным требованиям. В случае если количество срабатываний СПС из 18 экспериментов будет менее 17, то принимается решение о несоответствии показателя вероятности обнаружения заданным требованиям. В случае принятия такого решения, согласно методикам, могут проводиться повторные и/или дополнительные испытания после соответствующей настройки СПС по изменению порога чувствительности.

Теперь рассмотрим пример контроля нормативного значения средней наработки на ложное срабатывание в 600 часов. По новой методике необходимо проводить наблюдение за СПС в течение 63 часов (вместо 600 часов). Если ложных срабатываний за это время не было, то с риском поставщика и заказчика, равным 0.1, принимается решение о соответствии показателя наработки на ложное срабатывание заданным требованиям. В противном случае, если было хотя бы одно ложное срабатывание, принимают решение о несоответствии требованию при данных настройках порога чувствительности. При принятии решения о

Для оценки $T_{ложн}$ по методике контрольных испытаний время испытаний составляет 63 часа вместо 600 часов при использовании определительных методов.

несоответствии могут проводиться повторные испытания после соответствующей настройки СПС по изменению порога чувствительности.

Разработанные корпорацией «ПЕНТАКОН» методики контрольных испытаний периметральных систем (КИПС) построены на базе действующих ГОСТ Р 27.403-2005, ГОСТ 27.402-95 и могут быть использованы, во-первых, для приемо-сдаточных испытаний СПС различных производителей и на любых объектах, а, во-вторых, для сертификации систем. Для удобства и простоты использования методики КИПС предлагаются пользователям в виде диалоговой программы.

5
Стоимость СПС

5.1. Структура стоимости СПС

За безопасность необходимо платить, а
за ее отсутствие расплачиваться
Уинстон Черчилль

Очень часто представление о стоимости системы основывается на оценке стоимости оборудования базового элемента, тем более что функционально он одинаков для большинства систем. Кроме того, предполагается, что монтаж любой СПС и сопутствующие материалы будут стоить приблизительно одинаково. Поэтому считается, что какая бы система не была бы выбрана, ее стоимость будет определяться стоимостью оборудования. Однако это утверждение не совсем верно.

Говоря о затратах на СПС следует говорить о совокупной стоимости владения системой, которая включает затраты, связанные с приобретением, внедрением и эксплуатацией СПС.

Универсального метода расчета величины совокупной стоимости не существует, потому как структура затрат определяется видом самого объекта. Создаются индивидуальные методики, ориентированные на конкретный объект владения и применяемые отдельно для каждой стадии жизненного цикла. Для приблизительной оценки совокупной стоимости владения применяются упрощенные методики расчета, предполагающие существование двух видов издержек: прямые и косвенные. К прямым расходам относятся все

Стоимость СПС – это не только стоимость базового элемента.

траты, связанные с приобретением системы, а к косвенным – потери, связанные с обладанием активами (эксплуатацией), включая затраты на обучение и повышение квалификации сотрудников.

Очень упрощенно совокупную стоимость владения СПС можно оценить по формуле:

$$ССВ = С_{системы} + С_{эксп} + С_{об},$$

где:
ССВ – совокупная стоимость владения;
$С_{системы}$ – стоимость создания СПС;
$С_{эксп}$ – расходы, связанные с эксплуатацией СПС;
$С_{об}$ – расходы на обучение и повышение квалификации сотрудников, обслуживающих СПС.

5.2. Стоимость создания СПС

Стоимость создания СПС складывается из нескольких составляющих, которые могут учитываться или игнорироваться в оценочных расчетах.

Стоимость создания СПС можно рассчитать по формуле:

$$С_{системы} = С_{оборудования} + С_{материалов} + С_{монтажа},$$

где:
$С_{системы}$ – стоимость создания СПС;
$С_{оборудования}$ – стоимость элементов СПС;
$С_{материалов}$ – стоимость дополнительных материалов;
$С_{монтажа}$ – стоимость монтажа СПС.

При этом не учитывается стоимость ограждения и стоимость другого оборудования (стоимость системы охранного телевидения и т.п.).

Стоимость СПС сильно зависит от стоимости монтажных работ и дополнительных материалов.

Попробуем оценить доли затрат на оборудование СПС, монтаж системы (оценка стоимости монтажных работ проведена на основе СНиПов ФЕРм-10-04 и ФЕРм-10-08) и дополнительные материалы. Процентное соотношение долей стоимости основного оборудования, монтажа и дополнительных материалов (при одном бюджете) для систем на основе проводной радиолокации и трибоэлектрических систем будет выглядеть следующим образом (рис. 23):

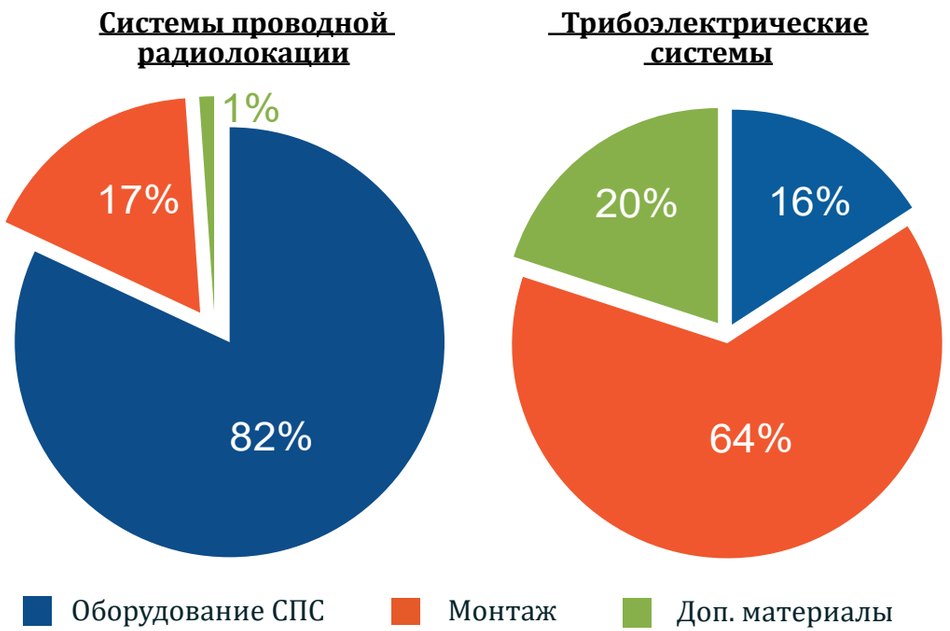


Рис. 23 *Распределение долей стоимости основного оборудования, монтажа и дополнительных материалов для различных систем*

Таким образом, СПС на основе проводной радиолокации (например, СТРАТУМ), имея стоимость базового элемента выше, чем у трибоэлектрических систем, выигрывает у них по стоимости монтажа и дополнительных материалов. И разница в стоимости системы увеличивается

при увеличении протяженности оборудуемого периметра, так как для трибоэлектрических систем резко возрастает стоимость монтажа и дополнительных материалов (рис. 24)

Совокупная стоимость создания СПС на основе проводной радиолокации ниже, чем у трибоэлектрических систем при длине периметра более 2-3 км.

С течением времени, стоимость оборудования, того или иного производителя, несомненно меняется, однако сам подход в организации системы остается прежним, а значит тенденция роста стоимости решения будет прежняя. Таким образом данный рисунок будет актуален (с точки зрения тенденций) при любой стоимости оборудования.

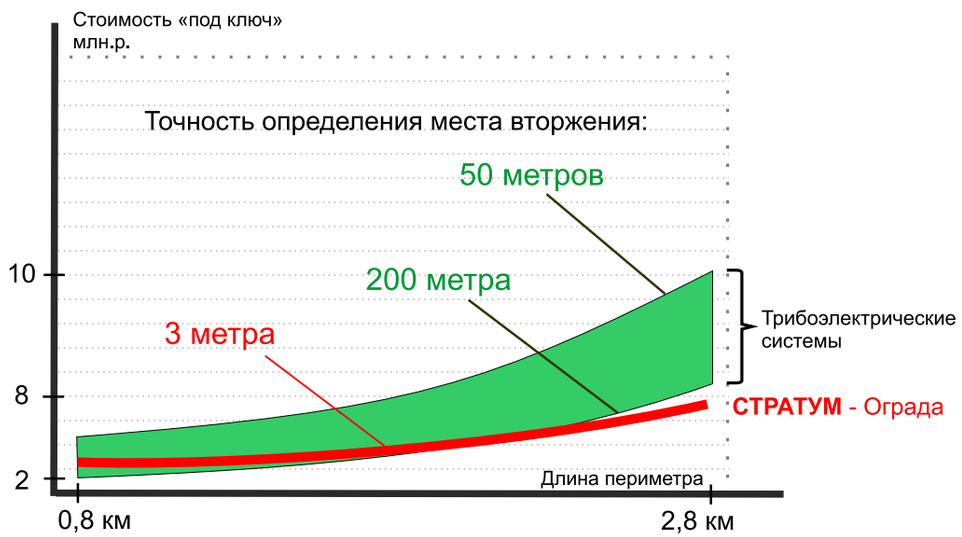


Рис. 24 *Зависимость стоимости различных систем от длины периметра*

5.3. Оценка стоимости владения

Безопасность это процесс, а не результат
Брюс Шнайер

Эксплуатационные расходы на СПС складываются из нескольких постоянных и переменных составляющих и зависят, в том числе, от времени наработки оборудования на отказ и его ремонтопригодности, а также частоты и стоимости проведения плановых работ (техническое обслуживание и текущий ремонт) и работ по сопровождению системы.

В приближенном виде стоимость эксплуатационных расходов можно представить как:

$$C_{эксп}=f(T_{отк}; R; W; t),$$

где:
$C_{эксп}$ - стоимость эксплуатационных расходов;
$T_{отк}$ - время работы на отказ;
R - ремонтопригодность;
W - плановые работы (техническое обслуживание и текущий ремонт) и сопровождение системы;
t - срок службы системы.

Частоту и стоимость проведения плановых работ (техническое обслуживание и текущий ремонт) и работ по сопровождению системы можно оценить исходя из положений ГОСТ Р 54101-2010 (с учетом других регламентирующих документов) и стандартных расценок на производимые работы.

Сложнее дело обстоит с другими параметрами, например, со временем наработки на отказ. Если судить о надежности основных бло-

ков систем, то, учитывая приблизительно одинаковую технологию их изготовления и используемые компоненты, разумно предположить, что она должна быть приблизительно одинаковой. Однако производители дают значение среднего времени наработки на отказ от 30 000 часов (3 года) до 60 000 часов (7 лет). Одновременно с электронными блоками должна оценивается и надежность трибоэлектрического кабеля (важная часть системы), который, как уже было сказано, при установке на АКЛ или колючую проволоку может выйти из строя через год-полтора.

Чем больше контактов и соединений в системе, тем выше эксплуатационные расходы и тем ниже надежность.

Если судить о надежности системы по общему числу контактов и соединений в системе (по числу наименее надежных элементов), то и в этом сравнении также лидирует система на основе проводной радиолокации, имеющая минимальное число блоков, кабелей и, следовательно, соединений. И действительно, есть опыт безотказной работы системы в сложных условиях (-47 °С…+45 °С) на протяжении более 10 лет.

К задачам сопровождения системы относятся, в первую очередь, коррекция настроек, в том числе сезонная калибровка, а также задание иной конфигурации зон охраны и взаимодействия подсистем. В системе на основе проводной радиолокации (например, СТРАТУМ), в отличие от других систем, эти процедуры выполняются на программном, а не на аппаратном уровне. И поэтому выполняются быстро, просто и дешево.

6
Как обучить персонал и не дать ему «угробить» систему

… ни одна система безопасности не устоит
против тупости собственных сотрудников
Стиг Ларссон

Изначально было указано, что инновационные комплексные системы безопасности призваны автоматизировать и облегчить труд сотрудников охраны. Однако и к персоналу, обслуживающему современные системы безопасности, предъявляются все более высокие требования.

К сожалению не все понимают, что обучение сотрудников служб безопасности и постоянное повышение их квалификации является одним из важных аспектов обеспечения безопасности предприятия. Можно сказать, что каждый рубль, вложенный в обучение персонала, может сэкономить, в буквальном смысле, миллионы.

В предыдущих разделах было показано, что сотрудники охраны, например, могут или настроить систему периметральной сигнализации так, что она не будет реагировать на большинство нарушителей или совсем ее отключить. Причем это может произойти не только из-за того, что сотрудник банально ленив, но и просто из-за его низкой квалификации. Поэтому, чтобы система безопасности не стала дорогой игрушкой или неким «экспонатом», следует производить подбор кадров, формирование службы эксплуатации и корректирование численного состава

Каждый рубль, вложенный в обучение персонала, может сэкономить, в буквальном смысле, миллионы.

службы охраны, а также обучение обслуживающего персонала еще до начала эксплуатации. Кроме того, должны быть разработаны нормативные акты, требования к сотрудникам в плане профессиональных навыков и компетенций, должностные инструкции и сценарии действий личного состава службы безопасности и сотрудников предприятия при штатных и нештатных ситуациях. В общем, должны быть решены следующие задачи:

1. подготовка нормативной документации;
2. подбор кадров, формирование служб, аттестация специалистов;
3. обучение обслуживающего персонала правилам эксплуатации комплекса;
4. разработка вводных задач, практических мер и сценариев действий личного состава службы безопасности к действиям при штатных и нештатных ситуациях;
5. контроль персонала, повышение его квалификации и переаттестация.

Примером нормативной документации, определяющей требования к специалистам и порядок аттестации, может служить «Положение по аттестации специалистов служб эксплуатации и обслуживания ИТСО и САЗ» ОАО «Газпром». Так, согласно указанному документу, в целях совершенствования теоретических знаний, практической подготовки, навыков и определения возможности предоставления права выполнять работы на объектах ОАО «Газпром», его дочерних обществ и организаций, все специалисты, осуществляющие деятельность по эксплуатации инженерно-технических систем охраны (ИТСО), в том числе и СПС, проходят обучение и аттестацию. Аттестации подлежат все специалисты, как вновь поступающие на работу, так и имеющие перерыв в работе в должности, предусматривающей эксплуатацию ИТСО более одного года. При этом предусмотрена и плановая аттестация, которая проводится периодически, но не реже одного раза в два года. Данный опыт, пожалуй, следует перенести на любое предприятие.

Аттестации подлежат все специалисты, как вновь поступающие на работу, так и имеющие перерыв в работе более одного года.

Кроме положения о квалификационных требованиях, порядке обучения и аттестации, должны быть разработаны специальные пособия по эксплуатации системы, возможных сбоях и неполадках и положения о действиях каждого специалиста в тех или иных штатных и нештатных ситуациях. Такое пособие должно разрабатываться совместно с разработчиком или инсталлятором и учитывать особенности конкретной СПС.

Специалисты по обслуживанию системы должны постоянно повышать квалификацию.

Обучение специалистов, эксплуатирующих КСБ, рекомендуется проводить на базе разработчика (на его полигоне или испытательном стенде) и/или непосредственно на объекте в присутствии представителей разработчика. Также могут быть задействованы сертифицированные учебные центры. Например, корпорация «ПЕНТАКОН», имеющая практический опыт разработки, построения и технического обслуживания систем обеспечения безопасности периметра, проводит курсы для специалистов по эксплуатации СПС, а также однодневные семинары для руководителей, принимающих решения, и проектировщиков систем (рис. 25).

Рис.25 *На занятиях в учебном центре «ПЕНТАКОНА»*

Кроме того, в рамках мероприятий по контролю работы персонала, необходимо, примерно раз в месяц, проводить практические занятия и учебные нарушения защиты. В этом случае разрабатывается сценарий учений, учитывающий принятые модели нарушителей и возможные нестандартные действия нарушителя, погодные и климатические условия, взаимодействие служб предприятия и сторонних организаций и т.д. По результатам учений корректируются модели нарушителей, положения о действиях служб предприятия, инструкции о мерах противодействия и т.д.

7
Центр компетенции по системам периметральной сигнализации

7.1. Задачи Центра компетенции по системам периметральной сигнализации

Если вы считаете, что компетентность стоит дорого, то попробуйте некомпетентность — она обойдётся вам гораздо дороже
Йохан Стаель фон Хольстайн

В 2014 году в Санкт-Петербурге корпорация «ПЕНТАКОН» открыла научно-технический Центр компетенции по системам периметральной сигнализации.

Основная объективная причина создания такого центра заключается в том, что системы защиты периметра, особенно периметра большой длины (например, в случае аэропортов) наиболее сложная в осуществлении часть КСБ. При этом ключевым и системообразующим элементом КСБ является СПС, от качества работы которой, в первую очередь, зависит эффективность охраны объекта. Насколько нетривиальна задача правильного выбора СПС было показано в предыдущих разделах.

Кому нужен сегодня Центр компетенции? Во-первых, заказчикам комплексных систем безопасности, которые могут получить консультации по вопросам выбора систем от специалистов Центра и провести экспертизу проектов. Во-вторых, проектировщикам, которые могут использовать в своих решениях методики проектирования сложных

КСБ, разработанные специалистами Центра. В-третьих, специалистам монтажных и эксплуатационных служб, которые могут повысить свою квалификацию на курсах и семинарах, проводимых на базе Центра компетенции.

Кроме того, сотрудники Центра могут провести приемо-сдаточные испытания и сертификацию уже смонтированных систем безопасности, используя разработанные Центром компетенции методики.

Сегодня основными задачами Центра являются:

1. проведение объективного и сравнительного анализа характеристик периметральных систем, представленных на российском рынке;
2. формирование методик и критериев, которыми следует руководствоваться при выборе систем защиты периметра;
3. разработка методик проектирования КСБ и моделирования их работы, в том числе разработка программно-аналитического комплекса (ПАК) АКИМ;
4. проведение независимой экспертизы проектных решений;
5. консультации, обучение, ликвидация технической безграмотности специалистов;
6. разработка и производство Комплексной Системы Безопасности СТРАТУМ.

7.2. Моделирование как надежное средство оценки эффективности систем безопасности

Как уже не раз упоминалось в разделах выше, различные виды объектов требуют разных подходов к организации систем физической защиты (СФЗ), а также в зависимости от объекта определяются цели и задачи системы.

На начальной стадии концептуального проектирования проводится анализ уязвимости объекта и оценивается эффективность СФЗ, определяются наиболее вероятные цели для злоумышленников, модели нарушителей, проводится оценка возможного ущерба и дается оценка уязвимости объекта и существующей системы безопасности. Результаты ложатся в основу ТЗ по проектированию системы. При этом для проектировщика охранных систем оценка качества создаваемого продукта очень важна, так как от этой оценки зависит реализация проекта.

Работы по анализу уязвимости и оценки эффективности СФЗ могут проводиться следующими способами:

1. экспертная оценка – оценка со стороны неких специалистов (ФСБ, специальные организации и т.д.). Минусом этого метода является то, что эксперт или группа экспертов вносят в оценку свое субъективное мнение, основанное на их личном опыте и знаниях;
2. натурные испытания – исследования построенного объекта на предмет проникновения посторонних лиц, возникновение ложных тревог и целесообразности применённых средств. Такое исследование, при должном подходе, дает наиболее качественный результат. Однако проверить систему до её физической реализации невозможно;
3. компьютерное моделирование – моделирование СФЗ с применением методов компьютерного имитационного моделирования.

Первый способ не всегда объективный, так как в экспертную комиссию попадают люди с разной квалификацией и разным опытом работы. Второй – слишком трудозатратный, да и оценить систему надо

до ее построения, а не после того, как она будет смонтирована на объекте. Наиболее интересен последний способ, который в сочетании с традиционной оценкой уязвимости объектов со стороны экспертов даст пользу на всех этапах создания системы физической защиты на объекте от концепта до подготовки к физической реализации.

Сегодня на рынке существует несколько программных средств позволяющих в той или иной степени (или на том или ином уровне) производить моделирование и оценку эффективности СФЗ. Все они имеют определенные достоинства и недостатки, проанализировав которые Корпорация «ПЕНТАКОН» приняла решение о создании инновационного инструмента для проектирования, моделирования и анализа систем безопасности – программно-аналитического комплекса (ПАК) АКИМ.

В данном комплексе производится оценка СФЗ на основе имитационных моделей функционирования технических средств, поведения нарушителя, тактик службы охраны, работы операторов и др. Проводятся вычислительные эксперименты, и набирается статистика для оценки уязвимости объекта со стороны нарушителя и выработки мер по противодействию. При этом учитываются все особенности охраняемого объекта, варианты тактики работы охраны, ее размещение на объекте и проч.

Такой подход позволяет оценить различные варианты построения системы защиты объекта в соответствии с техническим заданием в рамках выделенного бюджета и избежать возможных ошибок при ее проектировании.

Использование системы имитационного моделирования ПАК АКИМ дает возможность сократить финансовые и временные затраты на анализ защищенности исследуемого объекта и проектирование систем физической защиты. Комплекс также позволяет специалисту определить сбалансированную комплектацию системы физической защиты (как качественно, так и количественно), позволяющую избежать как избыточности, так и недоукомплектованности.

Тел.: +7 (812) 633-04-33
Факс: +7 (812) 633-04-37
E-mail: office@cctv.ru
www.cctv.ru

Виктор Михайлович Крылов,
Президент Корпорации ПЕНТАКОН,
кандидат технических наук, доцент.

Родился в 1950 г. в Ленинграде. В 1973 г. с отличием окончил Ленинградский политехнический институт по специальности «инженер-системотехник». После окончания института начал трудовую деятельность в том же институте и прошел путь от младшего научного сотрудника до доцента кафедры информационных и управляющих систем Санкт-Петербургского государственного политехнического университета. Является автором свыше 50 научных работ, двух авторских свидетельств. В 1995 г. основал ЗАО «Росси-СП» (ныне Корпорация ПЕНТАКОН).

Многолетняя успешная трудовая деятельность отмечена рядом престижных наград: Виктор Михайлович Крылов награжден медалью лауреата "Личность Петербурга", серебряной медалью «За укрепление авторитета российской науки» и медалью «В память 300-летия Санкт-Петербурга».

Является почетным членом Клуба кавалеров ордена Александра Невского.