



**Реферат к отчету о проведенном
исследовании
в программно-аналитическом комплексе
«АКИМ»**

ООО «ПЕНТАКОН»

197110, Россия, г. Санкт-Петербург, ул. Красного Курсанта 25 литера Д

Контакты | +7 (812) 633-04-33 | office@cctv.ru

Работа «Моделирование СФЗ нефтебазы» - это пример применения программно-аналитического комплекса (ПАК) «АКИМ» для создания «цифрового двойника» комплексной системы безопасности (КСБ) реального объекта – нефтебазы. На основе этого «цифрового двойника» оценивается качество и полнота защиты объекта. В отчете приведены результаты имитационного моделирования проникновения разного типа нарушителей с разными целями на этот объект. На основе полученных результатов моделирования предлагаются способы коррекции проекта КСБ.

В разделе 1 (вводный) рассмотрена постановка задачи по оценке основных тактико-технических характеристик КСБ охраняемого объекта.

Назначение КСБ любого объекта – служить эффективным оружием защиты объекта от несанкционированных действий нарушителей, подобно тому, как комплекс ПВО С-400 служит оружием защиты объекта от средств воздушного нападения. Поэтому их основные тактико-технические характеристики (ТТХ) звучат практически одинаково:

- вероятность обнаружения нарушителя – $P_{обн}$;
- вероятность нейтрализации нарушителя (для КСБ) или попадания в цель (для С-400) – $P_{нейтр}$;
- вероятность ложной тревоги (ложного пуска для С-400) – $P_{лож}$. Для КСБ чаще применяется производная величина - среднее время наработки на ложное срабатывание – $T_{лож}$.

Требования к этим ТТХ КСБ формируются заказчиком и экспертами на основе оценки уязвимости объекта и отражаются в требованиях технического задания (ТЗ) на создание КСБ. Однако при проектировании КСБ осуществить обоснованный выбор технических решений для выполнения требований ТЗ весьма сложно и даже невозможно, потому что:

- реальные ТТХ некоторых систем (в первую очередь систем периметральной сигнализации – СПС) можно определить только после их установки и пуско-наладки на объекте. На этапе проектирования можно рассматривать только диапазон их возможных значений;
- вероятность задержания нарушителя зависит не только от возможностей инженерно-технических средств охраны (ИТСО) и правильного срабатывания периметральной сигнализации, но и от действий сотрудников служб безопасности (их размещения, тактики действий и т.п.), от топологии объекта, от погодных условий и пр.

Выбор технических средств и решений при проектировании КСБ повсеместно требуется осуществлять на основе их эффективности, но при этом такая оценка доступна не всегда и не всем. Такая оценка должна быть чем-либо обоснована. Эта оценка может быть получена следующими способами:

1. Экспертная оценка – субъективная оценка неких специалистов.

2. Натурные испытания – натурные исследования качества и эффективности построенного объекта (КСБ или комплекса ПВО), на основании которых затем в систему вносятся необходимые коррективы. Такие исследования дают наиболее объективный результат, но они возможны только после создания системы. Так поступают при создании оружия (комплекса ПВО), но, к сожалению, не КСБ объекта. Поэтому ТТХ КСБ оказываются не такими, какие прописаны в ТЗ, а такими, какими они получились по факту создания, т.е. неизвестными. Их количественная оценка повсеместно

отсутствует. Т.е. в реальности (на сегодня) требования ТЗ и ТТХ лишь приблизительно могут соответствовать друг другу. И степень их соответствия неизвестна.

3. Компьютерное моделирование – имитационное моделирование работы КСБ на базе «цифрового двойника» объекта, в котором в ходе вычислительных компьютерных экспериментов многократно моделируется процесс проникновения нарушителя (модели нарушителя) в определенных условиях (модель погодных условий и т.п.) на территорию охраняемого объекта (модель, в которой задается топология, места расположения постов охраны и др.). Задаются также модели действий охраны, операторов, патрульной службы и т.д.

По результатам многократных (например, 10^3 - 10^4) компьютерных экспериментов получаются статистические результаты и вычисляются оценки ТТХ системы, определяются наиболее уязвимые участки для проникновения на объект, количественно оцениваются риски и многое другое.

В разделе 2 кратко описаны возможности комплекса «АКИМ».

«АКИМ» - это автоматизированный комплекс проектирования и моделирования КСБ, использующий методы имитационного моделирования, который позволяет:

- обоснованно принимать решения по выбору и размещению ИТСО, охраны и т.д. при проектировании КСБ;
- корректировать КСБ под определенные требования и задачи;
- проводить детальный количественный анализ уязвимостей как в целом по объекту, так и по отдельным его участкам;
- оценивать качество защиты объекта и т.п.

В разделе перечислены и кратко охарактеризованы используемые модели элементов системы безопасности и их характеристики, указаны параметры моделей нарушителя, группы реагирования, патруля, операторов и т.д.

В разделе 3 описана постановка задачи моделирования работы КСБ «цифрового двойника» объекта заказчика в виде трех моделей:

- М1 – на основании данных проекта системы безопасности нефтебазы;
- М2 – модель М1 с учетом реальных условий на объекте;
- М3 – модель М2 с учетом реалистичных характеристик СПС.

Каждая из моделей объекта рассматривалась для трех вариантов целей проникновения и моделей проникающего нарушителя (см. таблица 1).

Таблица 1. Варианты моделей с различными целями проникновения и моделями нарушителей

Версия	Цель нарушителя	Тип нарушителя
v1	Железнодорожная эстакада слива	Дилетант (вандал)
v2	Газовая котельная	Подготовленный (вор)
v3	Резервуарный парк хранения нефтепродуктов	террорист

В разделе 4 приведены результаты моделирования работы КСБ для всех вариантов моделей (всего 9):

- гистограмма распределения вероятностей нейтрализации нарушителя вдоль периметра (по участкам). Для примера, на рис.1 показана гистограмма для варианта v1, а на рис. 2 – для варианта v2 модели М3;
- для каждой из моделей приводится краткая сводная таблица средних по объекту вероятностных характеристик задержания нарушителя. Например, для варианта v1 модели М3 таблица выглядит следующим образом (см. таблица 2);
- иллюстрация всех возможных траекторий (по кратчайшему пути) проникновения к заданной цели на плане объекта с указанием результата исхода: успешная и своевременная нейтрализация (зеленый цвет) и несвоевременная нейтрализация (красный цвет). Пример, представлен на рис. 3.



Рисунок 1 – Гистограмма распределения вдоль периметра вероятностей нейтрализации вандала, проникающего к железнодорожной эстакаде слива (модель М3.v1)



Рисунок 2 – Гистограмма распределения вдоль периметра вероятностей нейтрализации вора, проникающего к газовой котельной (модель М3.v2)

Таблица 2. Вероятности обезвреживания нарушителя для цели «железнодорожная эстакада слива» и модели нарушителя «вандал» (М3.v1)

Минимальная вероятность обезвреживания, %	47.7% (участок: 18)
Средняя вероятность обезвреживания, %	77.4%
Обнаруживающая способность системы ТСО, %	90.9%
Минимальная задержка нарушителя на ИСО	24 сек.
Среднее время задержки нарушителя на ИСО	224,3 сек. (3 мин. 44 сек.)
Максимальное время задержки на ИСО	1171 сек. (19 мин. 31 сек)
Средняя задержка со стороны ИСО относительно времени затраченного на весь маршрут (X%)	90,3%

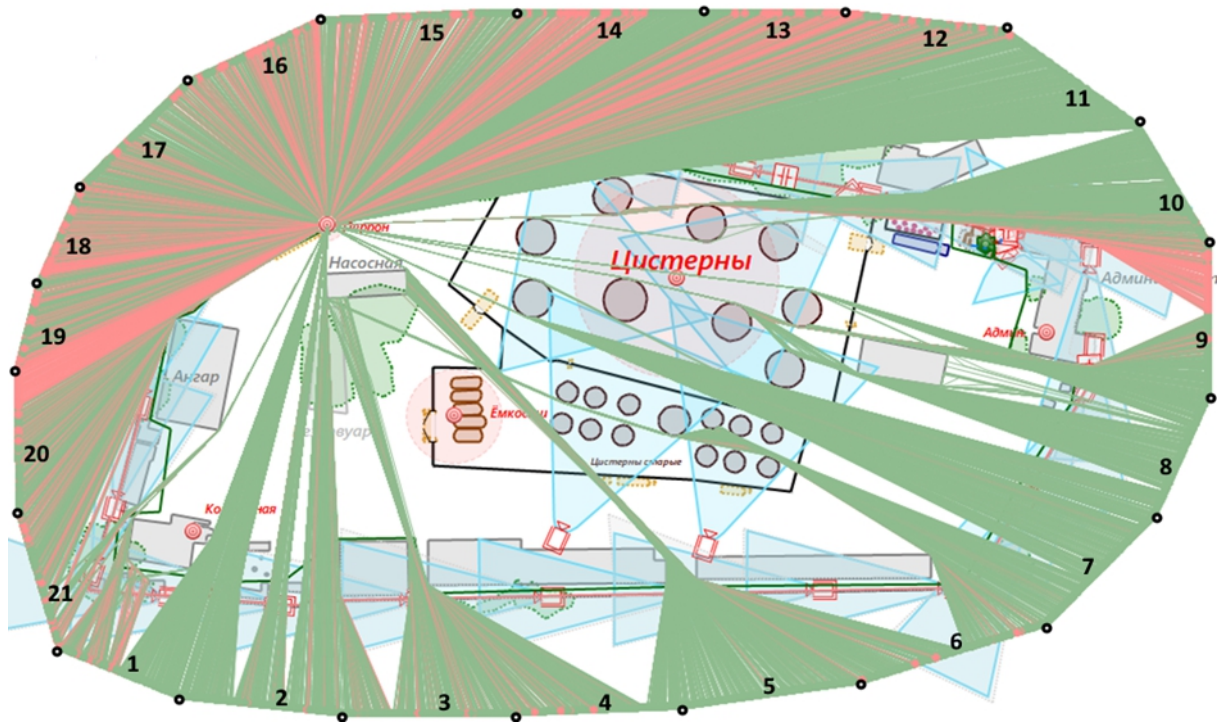


Рисунок 3 – Диаграмма траекторий проникновения для 10 000 испытаний для варианта v1 модели М3

Существуют более полные и подробные результаты по каждому из вариантов, но они в отчете не приводятся ввиду их большого объема. Краткая сводка результатов моделирования приведена в таблице 3.

Таблица 3. Краткая сводка результатов моделирования (в скобках – падение значений $P_{обн}$ относительно предполагаемых Заказчиком 100%)

Модель	Вероятности обнаружения и нейтрализации, %	Цели/нарушитель		
		жд эстакада/ вандал (v1)	газовая котельная/ вор (v2)	парк хранения нефтепродуктов/ террорист (v3)
М1 – проектная документация	$P_{обн}$	100	100	100
	$P_{нейтр}$	85	50.7	77.3 (-23%)
М2 – М1 (проект) + реальная местность	$P_{обн}$	97.3	97.8	100
	$P_{нейтр}$	83.5	46.8	74.8 (-25%)
М3 – М2+реальные характеристики СПС	$P_{обн}$	90.9	93.8	99.9
	$P_{нейтр}$	77.4 (-13%)	44.3 (-56%)	71.6 (-30%)

В главе 5 предложены возможные варианты коррекции КСБ и приведены результаты их моделирования (см. таблица 4):

- посредством установки дополнительных технических средств охраны (для жд эстакады);
- посредством изменения тактики работы людей (введение дополнительного поста охраны для газовой котельной).

В обоих случаях качественные показатели оценок КСБ значительно возросли (защищенность повысилась).

Таблица 4. Краткая сводка результатов моделирования модификаций КСБ (в скобках – изменение значений $P_{обн}$ и $P_{нейтр}$ относительно результатов моделирования модели МЗ)

Модель	Вероятности обнаружения и нейтрализации, %	Цели/нарушитель	
		жд эстакада/ вандал (v1)	газовая котельная/ вор (v2)
Исходная модель МЗ	$P_{обн}$	90.9	93.8
	$P_{нейтр}$	77.4	44.3
Коррекция МЗ: дополнительные ТСО	$P_{обн}$	100 (возросло на 9%)	-
	$P_{нейтр}$	97.5 (возросло на 20%)	-
Коррекция МЗ: доп. пост охраны	$P_{обн}$	-	95.5 (возросло на 1.5%)
	$P_{нейтр}$	-	90.7 (возросло на 46%)

Заключения и выводы по результатам моделирования КСБ объекта:

1. Вероятность обнаружения нарушителя – $P_{обн}$.

В современной практике проектирования ТЗ для КСБ определяет ее как средство обнаружить, а не задержать нарушителя. Отсюда и основная характеристика системы $P_{обн}$.

Определяется $P_{обн}$, в первую очередь, качеством работы ИТСО – системой периметральной сигнализации и CCTV, включая видеоаналитику и профессионализм работы операторов. В исходном проекте $P_{обн}$ близка к 100% для всех трех моделей (цель + нарушитель – таблица 3). Можно заключить, что, с позиции значения $P_{обн}$, созданный проект во всех рассмотренных вариантах целей и типов нарушителя хорошо, близко к 100%, решает задачу обнаружения нарушителя.

Было проведено моделирование для всех трех моделей с использованием не учтенных проектом, но реально существующих на объекте условий (густая растительность из кустарников и деревьев на объекте и дачные участки, расположенные в непосредственной близости). Из-за того, что в этом случае изменяются в худшую сторону зоны наблюдения ТВ-камер, результаты моделирования показали, что $P_{обн}$ уменьшается в среднем на 2.5-3% по каждой из целей (см. таблица 3). Это уменьшение неравномерно и на некоторых участках составляет до 7%. Такая обнаруживающая способность обеспечена использованием идеализированной модели видеоаналитики, но в реальности ситуация может быть явно хуже.

Еще одно моделирование было проведено с учетом не паспортных, а более реальных (сниженных) значений $P_{обн}$ для СПС. В результате показано, что реальная $P_{обн}$ в среднем снизилась на 1-10% для разных целей и типов нарушителей, а на некоторых участках падение составило до 34%. Пример такого падения представлен на рисунке 4.



Рисунок 4 – Гистограмма вероятности обнаружения по периметру при проникновении нарушителя к газовой котельной (вор)

2. Вероятность нейтрализации нарушителя $P_{нейтр}$

$P_{нейтр}$ определяется не только обнаруживающими свойствами ТСО (значениями $P_{обн}$), но и ИСЗ, задерживающими нарушителя, и, конечно, действиями самих охранников, их количеством, расположением постов охраны и т.п.

Значения $P_{нейтр}$ в ТЗ не указывается, поскольку в современной практике проектирования по умолчанию считается, что нарушитель будет 100% нейтрализован, как только будет обнаружен. То есть в ТЗ предполагается, что $P_{нейтр} \approx P_{обн}$. Но это, конечно же, не так, и моделирование это ясно показывает (см. таблица 3).

3. Сопоставление вероятностей обнаружения ($P_{обн}$) и нейтрализации ($P_{нейтр}$) нарушителя

Для всех исследованных моделей и во всех рассматриваемых условиях результаты $P_{обн}$ и $P_{нейтр}$ существенно отличаются: до 50% в среднем и до ~97% на отдельных участках. Причина состоит в том, что при моделировании учитываются и места расположения, и число постов охраны, и, разумеется, действия сотрудников. Поэтому, в отличие от сложившейся практики оценки проектов, моделирование показывает, что, несмотря на близкое к 100% значение $P_{обн}$, существуют участки периметра, проникновение нарушителя через которые, например, в 98% случаев будет успешным!

4. Коррекция проектов

Комплекс «АКИМ» позволяет не только оценить качество проекта, не только учесть реально существующие на объекте условия, качество и тактику работы охранников, но и оценить эффективность вариантов локальной коррекции КСБ (см. таблица 4):

- коррекция с помощью дополнительных ТСО увеличила в среднем по периметру $P_{обн}$ на 9%, а $P_{нейтр}$ – на 20%. Более детально это показано на рисунке 5;
- коррекция с помощью размещения дополнительного поста охраны увеличила в среднем по периметру $P_{обн}$ на 1.5%, а $P_{нейтр}$ – на 46%. Более детально это показано на рисунке 6.



Рисунок 5 – Наложение гистограмм вероятностей обезвреживания нарушителя для системы до модификации (оранжевый – МЗ.v1: жд эстакада/вандал) и после модификации (зеленый)



Рисунок 6 – Наложение гистограмм вероятностей обезвреживания нарушителя для системы до модификации (оранжевый – МЗ.v2: газовая котельная/вор) и после модификации (зеленый)

Заключения и выводы по возможностям комплекса «АКИМ»

Комплекс «АКИМ» - это универсальный инструмент, который:

- позволяет определять наиболее уязвимые места и оценивать эффективность КСБ и уязвимость объекта в целом;
- помогает подготавливать материалы для проектирования или модернизации КСБ;
- помогает оценивать различные варианты построения КСБ в рамках выделенного бюджета;
- помогает обоснованно определить минимально необходимый объем инженерно-технических средств охраны объекта, необходимый для защиты объекта с заданным в ТЗ качеством;
- помогает определить оптимальную структуру службы безопасности и необходимую численность сотрудников;
- помогает подготовить варианты оптимального размещения постов (караулов), путей и графиков движения патрулей по территории объекта;
- формирует информационно-аналитические материалы на основе результатов моделирования.

В тоже время, проведенное исследование показало, что комплекс «АКИМ» требует развития и совершенствования по следующим направлениям:

- повышение удобства использования комплекса для проектирования и моделирования;
- создание клиент-серверной версии программного комплекса;
- создание библиотеки стандартных элементов ИТСО и проектных решений;
- создание модуля для анализа проекта на соответствие требованиям законодательных и нормативных актов (в областях ТЭК, транспорта и др.);
- разработка модуля составления спецификаций ТСО и калькулятора примерной стоимости проекта/модификации проекта;
- повышение быстродействия (повышение уровня автоматизации и повышение скорости расчетов);
- создание базы данных реальных экспериментальных характеристик для СПС (ограждение + система извещателей);
- разработка модуля интеллектуального помощника;
- моделирование и анимация в 3D (сейчас используется 2D-проекция);
- моделирование проникновения дронов на территорию объекта;
- моделирование систем противодействия дронам;
- использование спутниковых карт для составления честных «цифровых двойников» охраняемых объектов;
- моделирование систем охраны многоэтажных строений (офисное здание с системой охраны и т.п.).