РЕАЛЬНОЕ КАЧЕСТВО СИСТЕМ ЗАЩИТЫ ПЕРИМЕТРА

(ЗА ЧТО ДОЛЖЕН ПЛАТИТЬ ЗАКАЗЧИК)

Крылов Виктор Михайлович

к.т.н., доцент,
Президент компании «ПЕНТАКОН»

ПЕНТАКОН
КОРПОРАЦИЯ

На слайде 1 представлены две системы защиты объекта: ЗРК С-400 и система защиты периметра (СЗП). Несмотря на значительную непохожесть, эти системы функционально решают одну и ту же задачу – не допустить проникновения нарушителя (разного для каждой из систем) на охраняемый объект. Для этого каждая из систем защиты должна обеспечить решение двух задач:

1. Своевременное и достоверное обнаружение нарушителя ($P_{обнаружения}$, $T_{ложное}$).
2. Нейтрализацию (задержание) нарушителя ($P_{нейтрализации}$).

Качество и эффективность решения этих задач определяются тактико-техническими характеристиками (ТТХ) системы защиты, которые для обеих систем звучат практически идентично.

Системы защиты объекта

Система ПВО (ЗРК)

ТТХ:

$P_{обнаружения}$ нарушителя

$P_{ложного}$ пуска (ложной тревоги)

$P_{поражения}$ нарушителя

Система защиты периметра

ТТХ:

$P_{обнаружения}$ нарушителя

$P_{ложной}$ тревоги ($T_{ложн.}$)

$P_{нейтрализации}$ нарушителя

Обязательно задание всех трех ТТХ

1. Чтобы система защиты была бы таковой, необходимо задать и обеспечить все три основные ТТХ. Если не задана или задана на низком уровне хотя бы одна из трех вероятностных ТТХ, то система (ЗРК или СЗП) не может рассматриваться как система защиты объекта. Например, если ЗРК не обнаруживает (плохо обнаруживает) нарушителя ($P_{обнаружения}$ мала), то зачем тогда этому ЗРК хорошие ракеты?

2. По заданным ТТХ заказчик ЗРК покупает уже готовый комплекс.

3. В случаях, когда ТТХ системы (ЗРК или СЗП) не задаются (неизвестны или известны только частично), разумно предпочесть приобретение имитатора или муляжа системы защиты. Например, в случае ЗРК 3 при этом достигается сопоставимый психологический эффект за 1/1000 стоимости системы.

К сожалению, в случае СЗП дела обстоят по-другому: имитатор системы выглядит как сама система.

ЗРК — готовый типовой комплекс

1. Задай ТТХ:

$P_{обнаружения}$ нарушителя

$P_{ложного}$ пуска (ложной тревоги)

$P_{поражения}$ нарушителя

2. Выбери модель

Стоимость 100%

1. ТТХ не задают

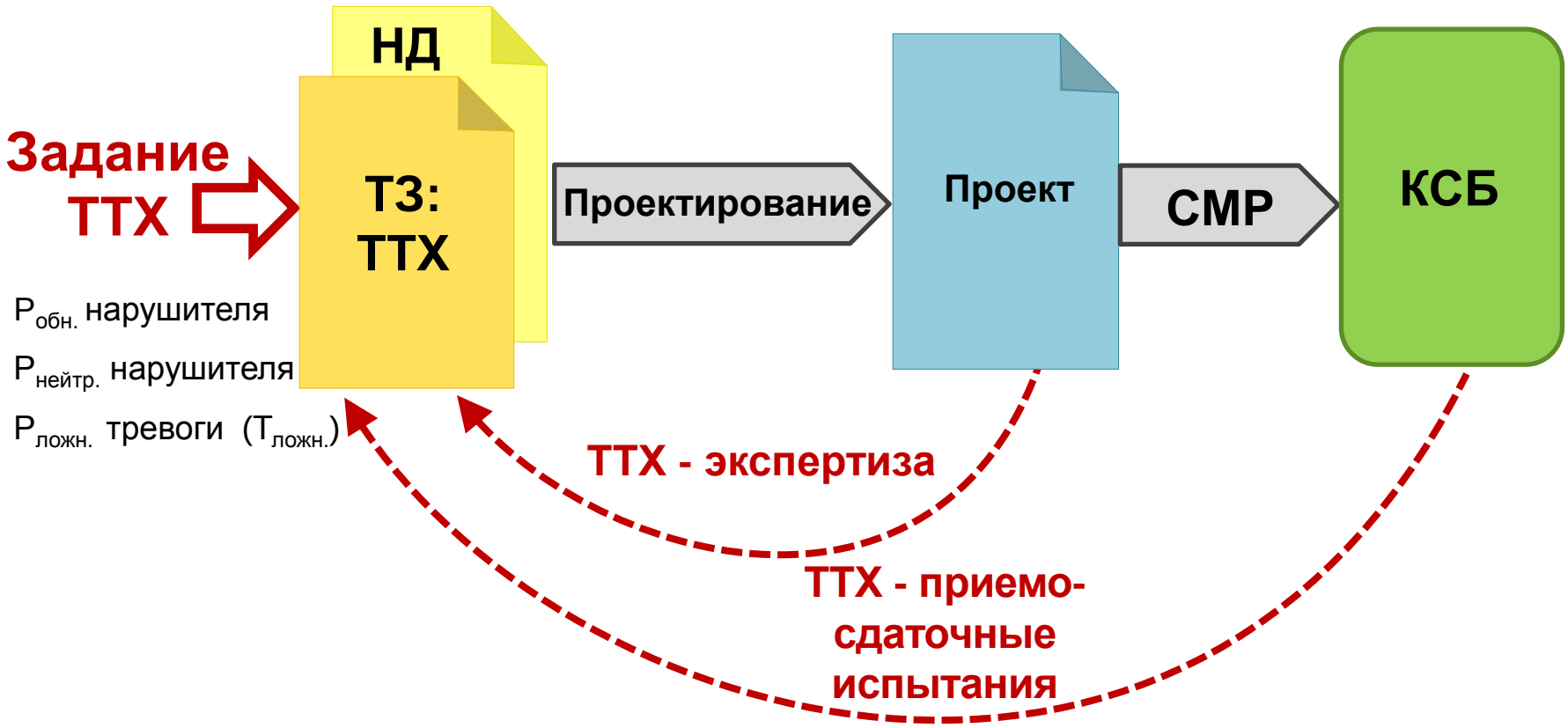
2. Выбери муляж ЗРК

Стоимость ~0.1%

В отличие от ЗРК всякая система безопасности, и система защиты периметра (СЗП) в частности, реализуется только по индивидуальному проекту. Проект повторного применения невозможен.

Все три заданные ТТХ должны контролироваться на этапе экспертизы проекта и в ходе статистических приемо-сдаточных испытаний (ПСИ).

Система защиты периметра — всегда новый продукт

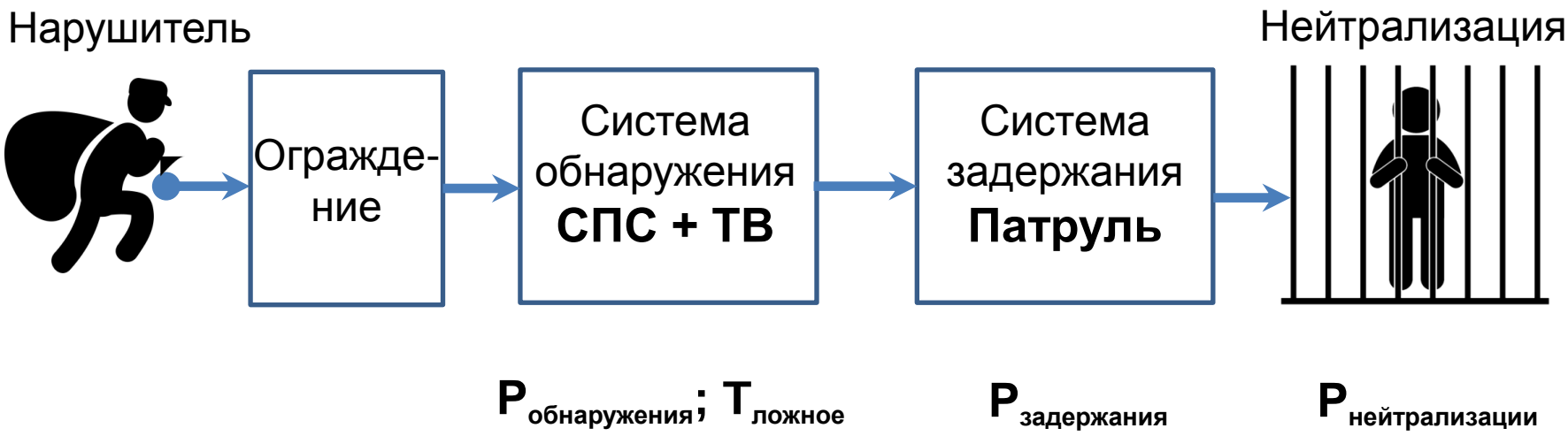


Типового проекта системы безопасности не существует.

Система обнаружения состоит из системы периметральной сигнализации (СПС) и расположенной вдоль периметра вспомогательной ТВ-системы. Успех в нейтрализации нарушителя обеспечивается не только высокой вероятностью обнаружения нарушителя $P_{обнаружения}$, но и эффективной и синхронной работой службы задержания.

Рассмотрим, как эти требования реализуются на практике.

Система защиты периметра (СЗП)



$$P_{нейтрализации} = P_{обнаружения} * P_{задержания}$$

1. Типовое ТЗ вообще не содержит никаких требований к подсистеме задержания (нейтрализации) нарушителя. Это означает по умолчанию, что $P_{задержания} = 1$. Фактически требования ТЗ предполагают, что подсистемы обнаружения нарушителя и его задержания работают независимо друг от друга. К сожалению, именно так и происходит на практике. Поэтому нет ничего удивительного в том, что реальное значение $P_{обнаружения}$ СПС может быть любым, что мы увидим далее. Любым, потому что ответственность за нейтрализацию нарушителя полностью переносится на подсистему его задержания, а от качества работы СПС зависит мало. На практике качество работы СПС оценивается как «хорошо/плохо».

2. Во всех ТЗ не требуется проведения статистических приемо-сдаточных испытаний с целью подтверждения заданных ТТХ. Уже хотя бы только по этой причине (есть и другие) реальные значения $P_{обнаружения}$ могут значительно отличаться от заданных в ТЗ.

Требования к системе защиты периметра

Типовое ТЗ	Реально
1. Требования к $P_{задержания}$ — нет Считается $P_{задержания} = 1$	1. $P_{задержания}$ — неизвестна $P_{задержания} \neq 1$
2. $P_{обнаружения} > 0.95$	2. $P_{обнаружения}$ — неизвестна
3. $T_{ложное} >$ 1/мес. … 1/год	3. $T_{ложное} \sim$ 1/сут. … 1/мес.

В таблице приведены результаты статистических испытаний реальных систем периметральной сигнализации. За исключением СПС «СТРАТУМ» у всех других систем значения $P_{необнаружения} = 1 - P_{обнаружения}$ кратно (у некоторых почти на 2 порядка) хуже заявленных в документации. Основные причины такого положения дел названы выше:

- размазывание ответственности за результат (за нейтрализацию нарушителя) в значительной степени перекладывая ее на службу задержания. При этом внятных количественных требований к качеству работы службы задержания не задается;
- повсеместно не проводятся статистические приемо-сдаточные испытания (ПСИ) СПС.

Для вибрационных СПС (80 % всех СПС в мире) указывать в документации конкретное значение $P_{обнаружения}$ вообще не корректно, так как оно определяется только в ходе пуско-наладочных работ непосредственно на объекте (см. следующий слайд).

Как следует воспринимать значения $P_{обнаружения}$ в документации? Два варианта ответа.

1. В большинстве случаев производитель указывает то, что желает Заказчик. В ТЗ записано $P_{обнаружения} > 0,95$ – пожалуйста, получите. Кое-кто (например, для системы «С6») утратив здравый смысл вообще заявляет, что $P_{обнаружения} = 100\ \%$, $P_{пропуска} = 0\%$.
2. Реже (например, «СТРАТУМ»): указанное значение $P_{обнаружения} > 0,98$ следует рассматривать как нижнюю границу возможных значений $P_{обнаружения}$.

Результаты испытаний СПС

Система	Тип	В документации		Результаты испытаний	
		$P_{обнаружения}$	$P_{необнаружения}$	$P_{обнаружения}$	$P_{необнаружения}$
С1	трибо	-	-	0.24	76%
С2 (3 испытания)	трибо	0.95	5%	0.62	38%
С3	вибро датчики	> 0.99	< 1%	0.20	80%
С4	трибо	0.98	2%	0.53	47%
С5	трибо	0.98	2%	> 0.85 (2 канала)	< 15%
С6	трибо	1.0	0%	-	-
СТРАТУМ (13 испытаний)	проводная РЛ	> 0.99	< 1%	> 0.997	**<0.3 %**

Любая СПС вибрационного типа вне зависимости от используемого физического принципа состоит из 3-х функциональных частей:

- ограждения (мембраны), вибрирующего под действием нарушителя;
- сенсора (трибо, пьезо, и т. д.), преобразующего механические колебания в электрический сигнал;
- блока обработки (программы), ключевым элементом которого является задатчик уровня чувствительности V. Этот уровень устанавливается индивидуально для каждой зоны сенсора (датчика) в процессе пуско-наладки системы на объекте.

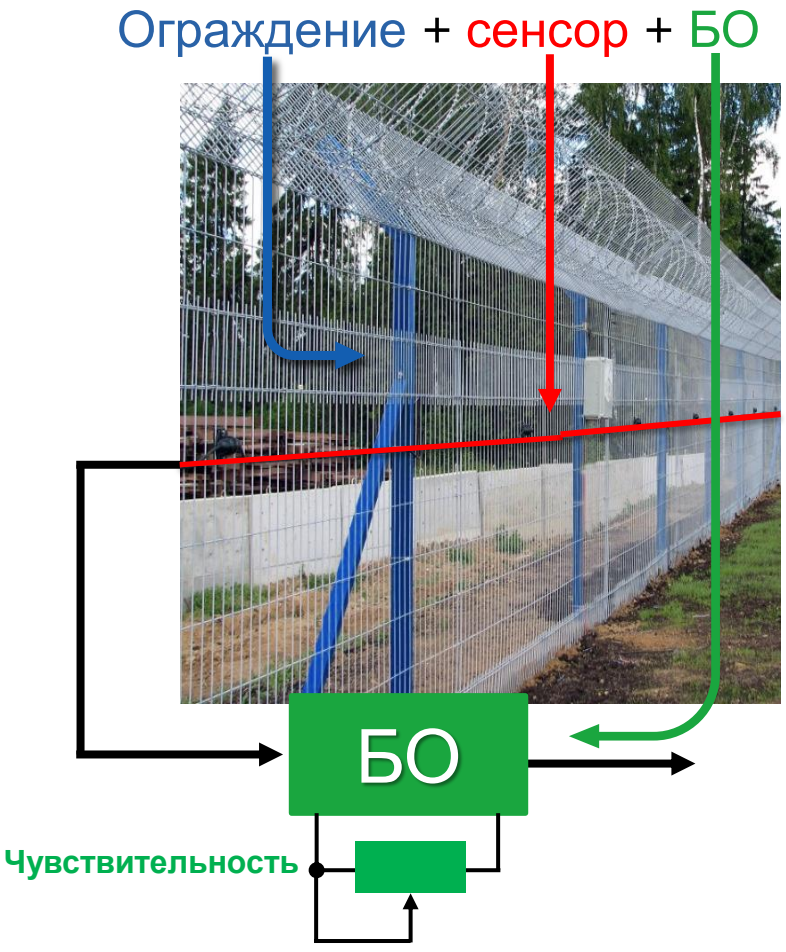
Совершенно очевидно, что для таких систем однозначно указывать в документации $P_{обнаружения}$ абсурдно с точки зрения здравого смысла.

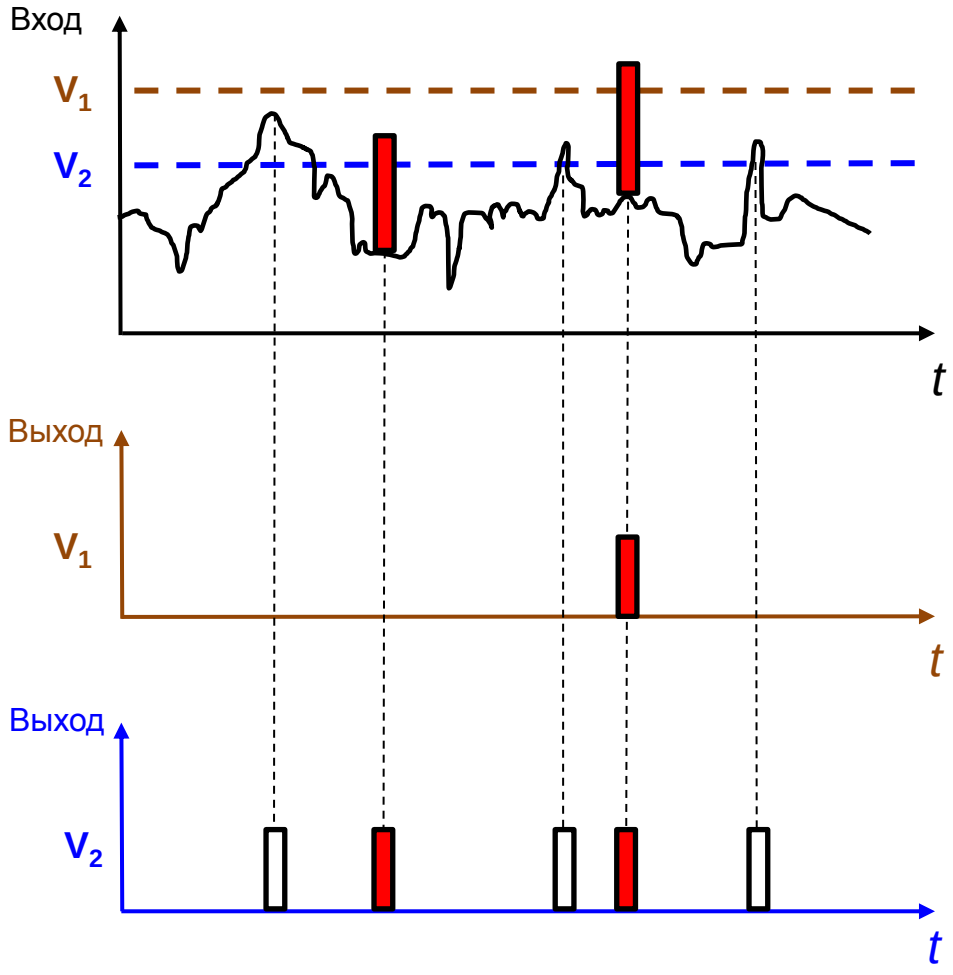
С другой стороны, если производитель оборудования не укажет значение $P_{обнаружения}$, то ни один заказчик или проектировщик СПС это оборудование никогда не выберет: ГИП должен обосновать выбор оборудования, исходя из требований ТЗ обеспечить $P_{обнаружения.}$ Поэтому производитель оборудования указывает именно то значение, которое вписывает в ТЗ Заказчик: $P_{обнаружения} > 0{,}95$. И ввиду повсеместного отсутствия статистических ПСИ эта «туфта» остается необнаруженной.

В процессе пуско-наладки из 2-х значений V_1, V_2 выбирается V_1. Число ложных срабатываний легко оценивается и устанавливается в соответствии с требованием ТЗ. Ну, а значение $P_{обнаружения}$ не оценивается, поэтому будет такое, какое получится. Реальное значение $P_{обнаружения}$ никому не известно, поскольку статистические ПСИ не проводятся.

$P_{обнаружения}$ задают на объекте

80% СПС – вибрационного типа:





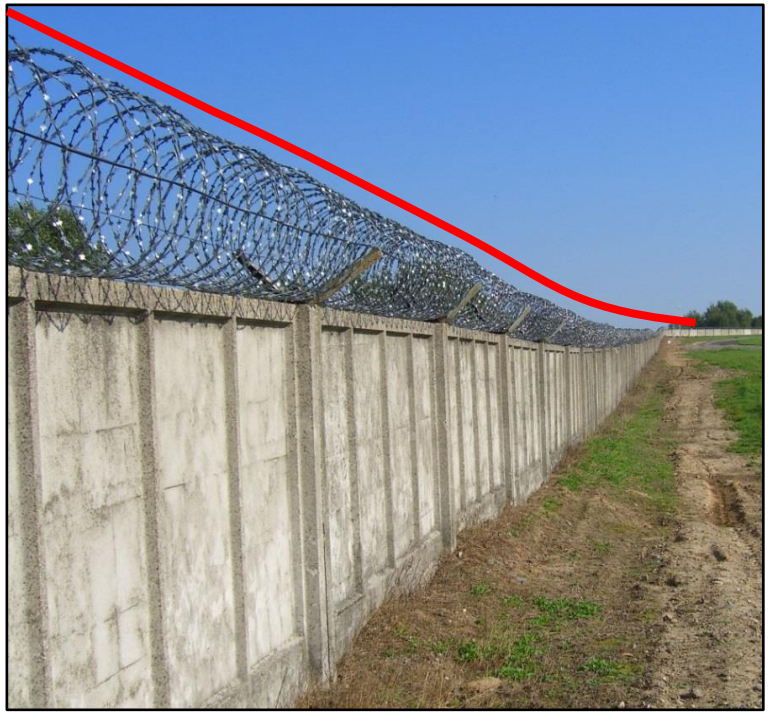
В некоторых случаях бессмысленность «системы», построенной за десятки миллионов рублей, становится видна невооруженным глазом. Ну какой нарушитель, если он не на танке, заставит вибрировать бетонный забор?

Не требует доказательств, что приведен пример не системы сигнализации, а пример бессмысленной и дорогостоящей ее имитации. Однако, основания предъявить претензии за эту имитацию к кому-либо отсутствуют. Формально правильно выбрано оборудование «С1», которое согласно документации, позволяет располагать сенсорный кабель на бетонном ограждении. Проект прошел экспертизу. Оборудование исправно функционирует.

Получается, что сегодня, в условиях отсутствия статистических ПСИ, отсутствует и чья-либо ответственность за результат и за создание подобных бессмысленных и дорогих аттракционов. Сложившееся положение дел, во-первых, вызывает сожаление о напрасно потраченных десятках млн. руб. (и это только на 1 объект) и, во-вторых, вызывает тревогу персональная ответственность у руководителей объекта.

Пример: Аэропорт Минеральные воды

Проект СПС
(на базе «СТРАТУМ»)



Имитация СПС
(на базе системы «С1»)

Проверки функционирования – **«ДА»**
ПСИ – **«НЕТ»**

Стоимость **системы (100%)**:
70.0 — 90.0 млн. руб

Стоимость **имитатора системы (100%)**:
70.0 — 90.0 млн. руб

На слайде кратко подведены основные итоги проведенного рассмотрения. К этому необходимо добавить, что всякая система защиты периметра строится по индивидуальному проекту в соответствии с её ТТХ. Поэтому в каждом случае требуется эффективный подбор оптимального варианта решения.

Реальное состояние систем защиты периметра

Существующие сегодня системы защиты периметра объектов не могут в полной мере считаться оружием защиты объекта потому что:

1. Типовые требования ТЗ неполно определяют ТТХ системы защиты периметра (требования только к СПС).
2. ТТХ системы не обосновываются и задаются на основе субъективных оценок экспертов.
3. Реальные значения ТТХ систем периметральной сигнализации в разы хуже заданных в ТЗ и не соответствуют значениям, указанным в документации на оборудование.
4. Статистические приемо-сдаточные испытания СПС и в целом СЗП повсеместно не проводятся.

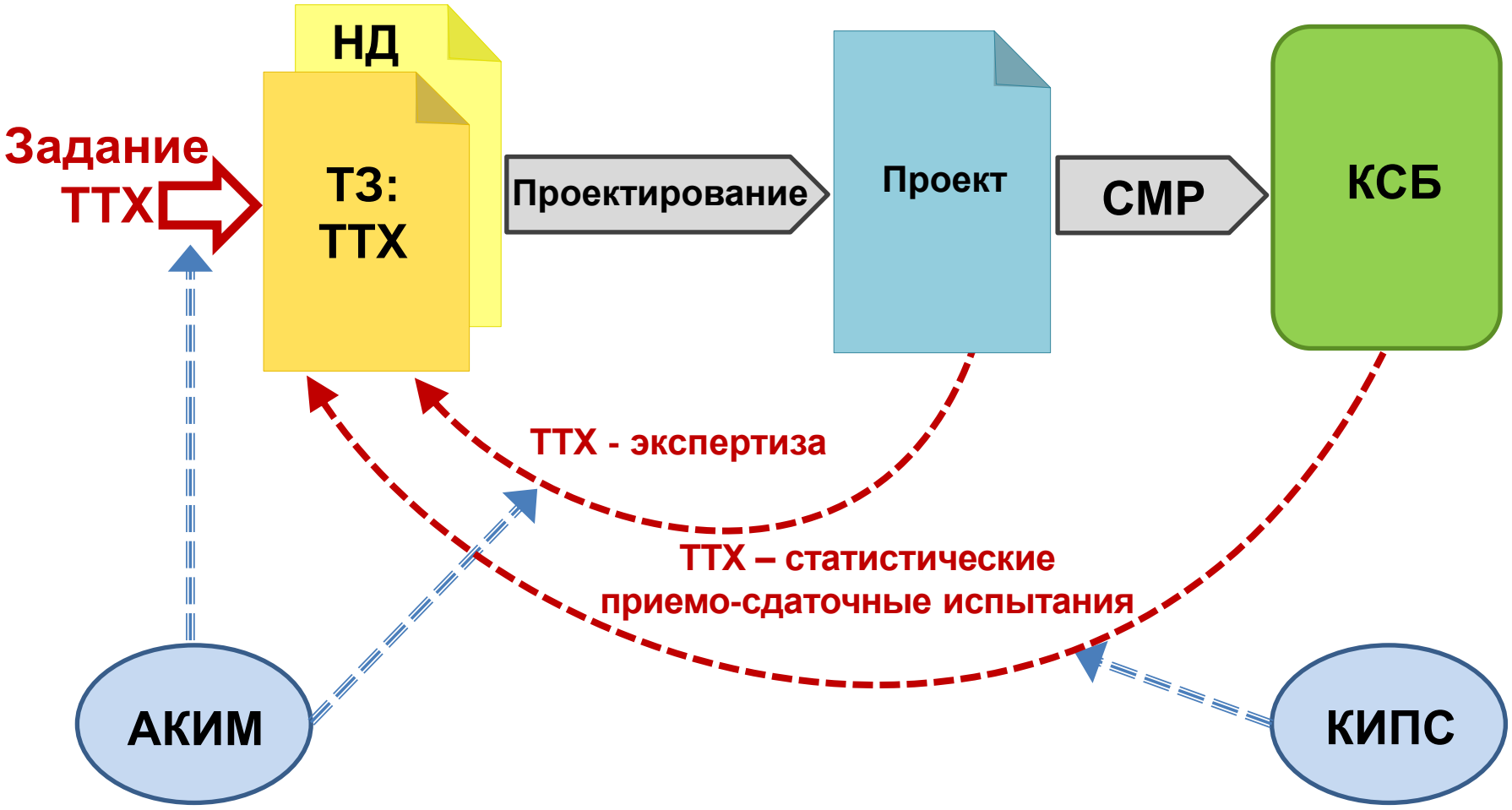
Чтобы создаваемая система защиты периметра являлась бы полноценным оружием защиты этого объекта необходимо обеспечить:

1. Обоснованное и полное задание основных ТТХ системы.
2. Выбор оптимального варианта ее построения, который должен включать не только выбор и расстановку технических средств, но также и определение расположения постов охраны, тактику ее работы и прочее.
3. Обязательное проведение статистических приемо-сдаточных испытаний системы периметральной сигнализации.

Для реализации этих требований компания «ПЕНТАКОН» предлагает:

1. Для решения задач 1 и 2 - аналитический комплекс «АКИМ», предназначенный для создания цифрового двойника системы безопасности. Моделирование позволяет находить оптимальное решение задач и обеспечивать полную и объективную экспертизу проекта.
2. Для решения задачи 3 - эффективные методики контрольных испытаний «КИПС», основанные на действующих ГОСТах.

Этапы создания системы безопасности

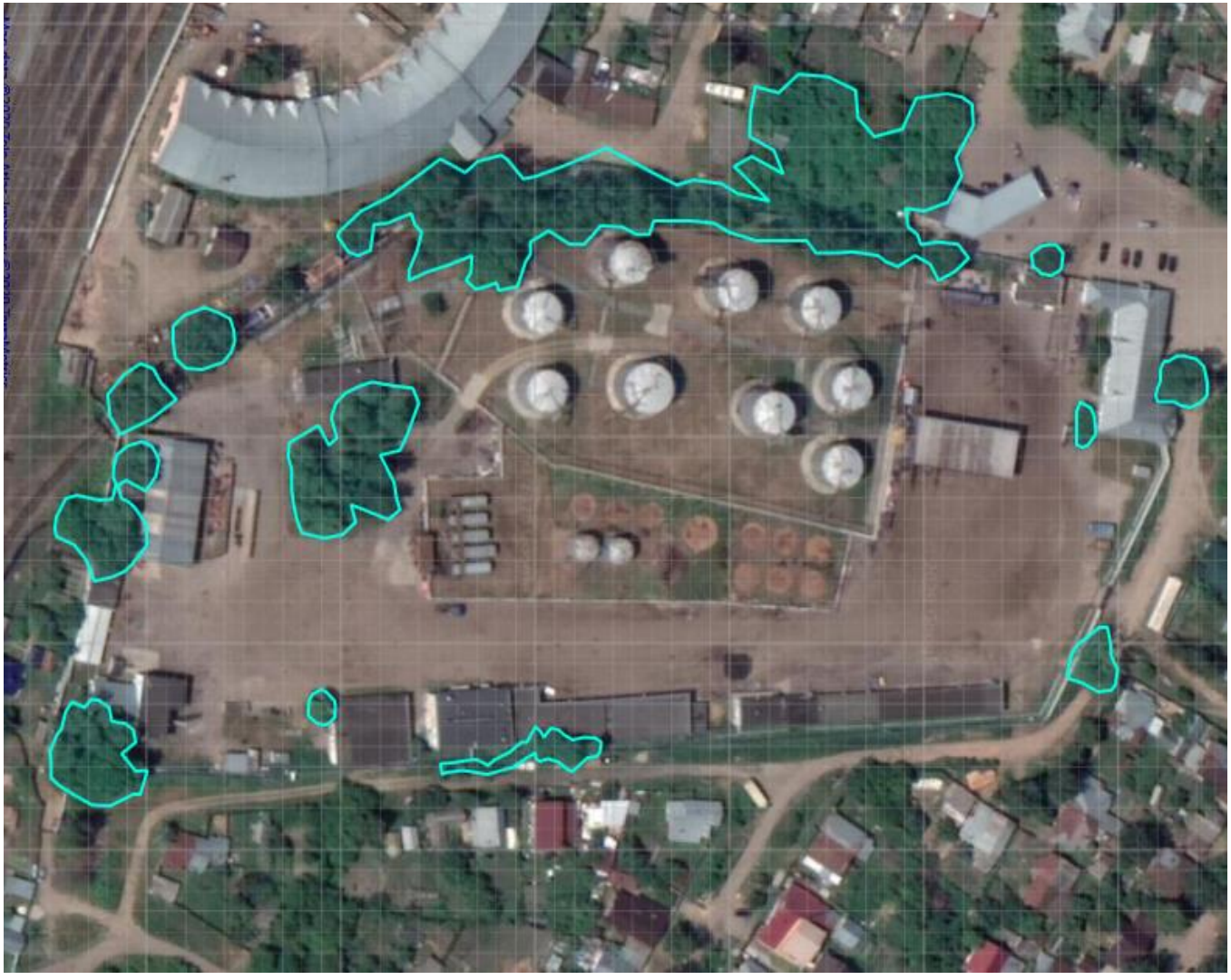


Кратко рассмотрим пример моделирования работы системы безопасности реального объекта.

Исходная информация для моделирования:

- готовый проект (AutoCAD);
- карта (Googlemap или иная).

Пример моделирования: нефтебаза

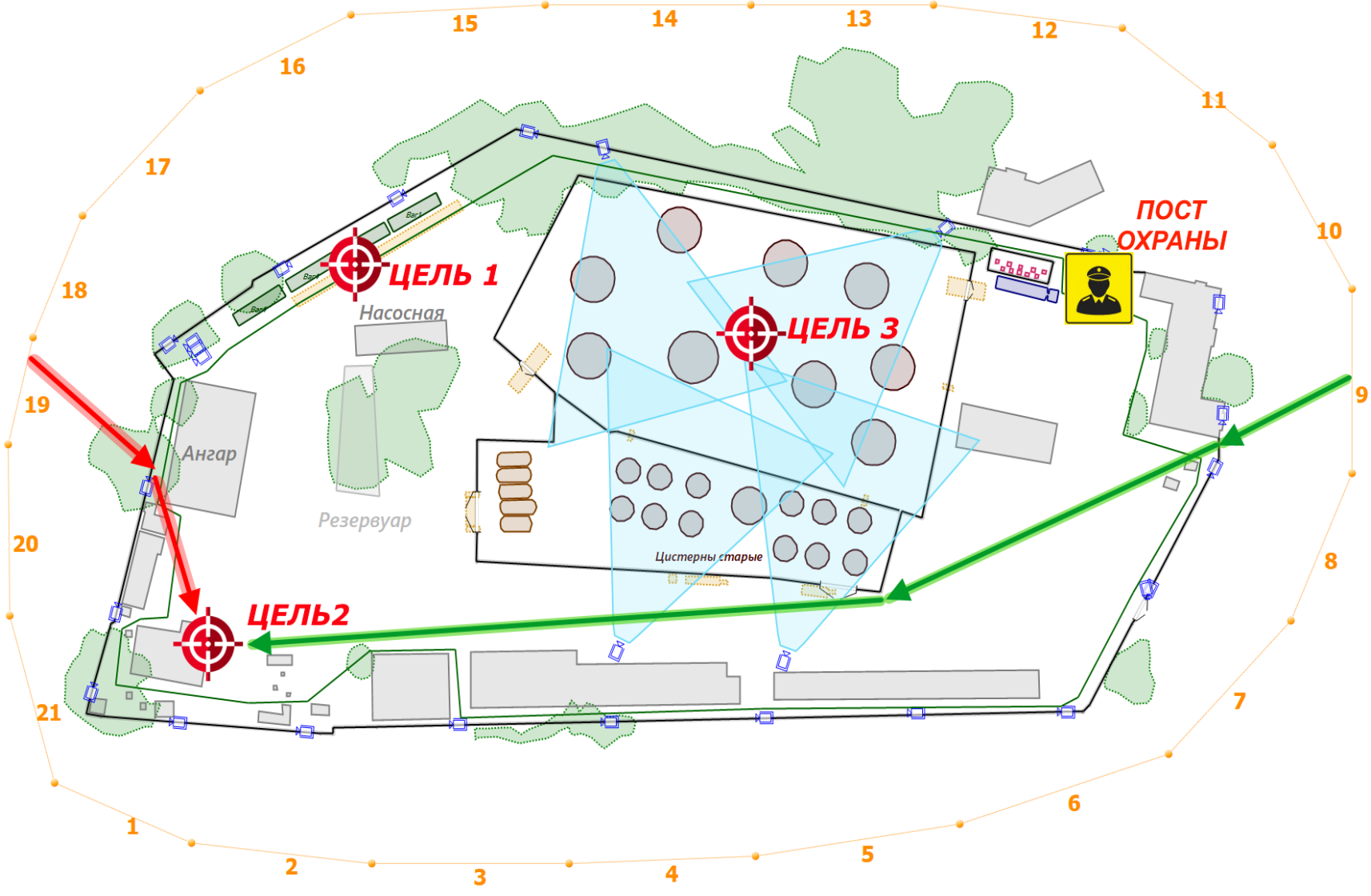


На плане располагаются:

- ограждения территории объекта;
- здания, сооружения, особенности местности;
- размещенные ТС (сигнализация, ТВ…);
- посты охраны.

Обозначаются цели, к которым будет стремиться нарушитель. Очевидно, что успех его задержания зависит от той точки, к которой он стремится. Зеленая линия – нарушитель не достиг цели (т.е. задержан). Красная линия – нарушитель своевременно не перехвачен.

Пример моделирования: план объекта



По результатам 10 000 попыток проникновения с разных направлений получены гистограммы вероятности обнаружения $P_{обнаружения}$ (почти везде близко к 100 %) и вероятности его нейтрализации $P_{нейтрализации}$. Есть участки периметра, где вероятность нейтрализации нарушителя 2-3 % при практически 100 % вероятности его обнаружения. Существование такого эффекта сегодня не обсуждается даже теоретически: считается, что если нарушитель обнаружен, то он 100 % и задержан.

Цифровая модель позволяет найти вариант оптимальной коррекции системы защиты объекта. В данном примере размещение еще одного поста охраны (увеличение стоимости системы менее 1%) сделала ТТХ системы приемлемыми.

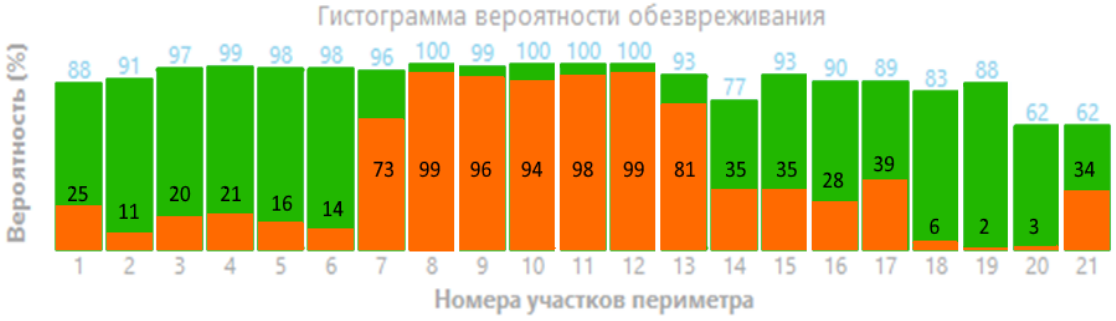
Пример моделирования:
результаты 10^4 попыток

Вероятность обнаружения нарушителя на участках периметра

$P_{обн.средн.} = 93.8\%$

ДО корректировки КСБ
Вероятность нейтрализации нарушителя

$P_{нейтр.средн.} = 44.3\%$



ПОСЛЕ корректировки КСБ
Вероятность нейтрализации нарушителя

$P_{нейтр.средн.} = 90.62\%$

Увеличение стоимости системы до 1%

Для проведения статистических приемо-сдаточных испытаний компания «ПЕНТАКОН» предлагает разработанные на основе действующих ГОСТов цифровые методики «КИПС».

Методики оформлены как программный комплекс, который позволяет в диалоговом режиме сформировать конкретные планы испытаний, произвести необходимые вычисления и оформить соответствующие протоколы.

Методики контрольных испытаний позволяют в десятки раз сократить объем необходимых экспериментов.

Решение ПЕНТАКОН: методики КИПС

Контрольные испытания на основе ГОСТ Р 27.403 – 2009

ГОСТ 27.402 – 95 и др.

1. Обоснование выбора участка для ПСИ.
2. Обоснование выбора способа преодоления.
3. Составление плана контрольных испытаний.
4. Автоматическое формирование протоколов.

Компания «ПЕНТАКОН» предлагает:

1. Цифровой комплекс «АКИМ» для обоснования ТТХ систем защиты периметра и КСБ в целом.
2. Цифровые методики «КИПС» для статистических приемо-сдаточных испытаний СПС.
3. Лучшую в своем классе систему периметральной сигнализации «СТРАТУМ».
4. Создание систем безопасности «под ключ».

ПЕНТАКОН
КОРПОРАЦИЯ

WWW.CCTV.RU OFFICE@CCTV.RU +7 (812) 401-41-33

197198, г. Санкт-Петербург,
ул. Красного Курсанта, дом 25, литер «Д»