СИСТЕМА ЗАЩИТЫ ПЕРИМЕТРА:

КАК ИСПОЛНИТЬ ЖЕЛАНИЕ ?

Крылов Виктор Михайлович

Президент компании «ПЕНТАКОН»

к.т.н., доцент

ПЕНТАКОН

КОРПОРАЦИЯ

Наша задача

СОЗДАЕМ ОРУЖИЕ ЗАЩИТЫ!

Базовое определение теории управления:

«Управление есть целенаправленный процесс изыскания и реализации мер по переводу объекта управления из текущего состояния в желаемое».

Поэтому первым шагом решения задачи создания системы безопасности объекта является формирование и разработка желаемого образа системы.

Пример образа желаемой системы безопасности на следующей странице.

Уверен, что любой сотрудник службы безопасности с удовольствием согласится, что именно такие условия работы должна обеспечивать желаемая система безопасности. Вот только кто возьмётся строить систему по такому техническому заданию?

Сегодня существуют два варианта:

1. Волшебная палочка или золотая рыбка.
2. Компания «ПЕНТАКОН».

Обсудим компетенции и know-how компании «ПЕНТАКОН».

Рассмотрим примеры двух систем защиты объектов.

«ЖЕЛАЮ, ЧТОБЫ ВСЕ!»

Цитата www.youtube.com/watch?v=ZaFz2APs4co

Обратите внимание, что ТТХ изображенных систем даже называются практически одинаково. Совершенно очевидно, что было бы глупо задавать для ЗРК и рассматривать как независимые три его главные ТТХ: $P_{обн.}$, $T_{ложн.}$, $P_{поражен}$. Например, если $P_{обн.}$ мала, то даже самые замечательные ракеты не обеспечат поражение цели. И наоборот, если $P_{обн}$. ~ 100% , а средства поражения слабы, то какой тогда смысл в 100% обнаружении цели?

Совершенно аналогично обстоят дела и в СЗП. Если, например не принимать в расчет или рассматривать независимо тактику работы и расположение постов охраны, то несмотря на замечательную работу СПС, даже при 100% обнаружении, главная задача по нейтрализации нарушителя может оказаться невыполненной. Необходим комплексный анализ СЗП для формирования ТТХ на СО.

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

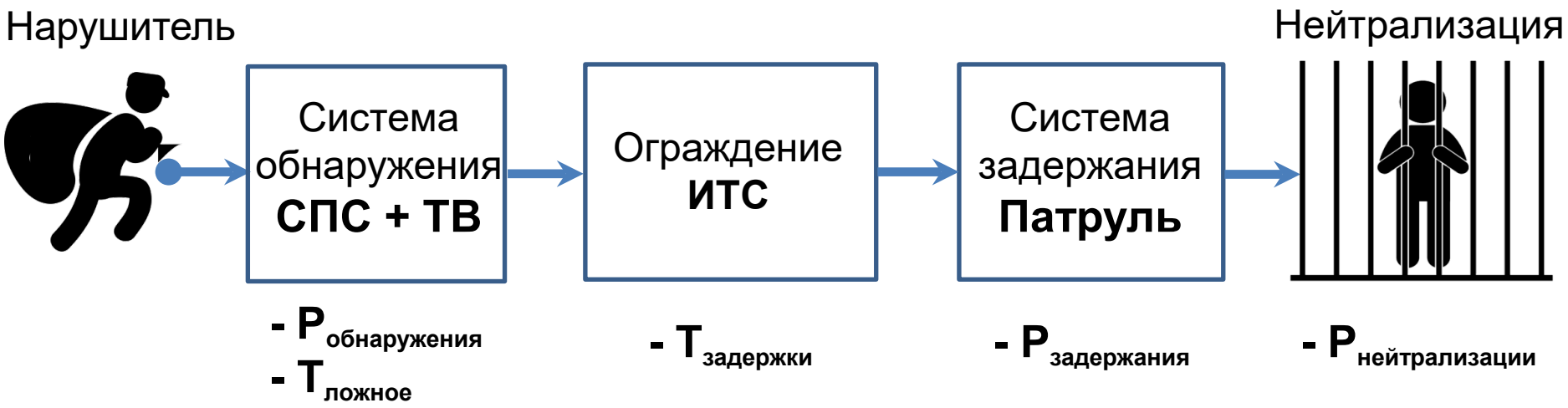
Обязательно задание всех трех ТТХ

Однако, практика сегодняшнего дня такова, что заказчик вместо одного ТЗ на всю систему защиты периметра обычно формирует три ТЗ на три подсистемы: ИТС, СПС, патрульно-охранная служба. Затем эти подсистемы проектируются и реализуются как независимо функционирующие, что в корне неправильно.

СПС является только частью, хотя и важнейшей СЗП. Задача СЗП – нейтрализовать нарушителя. Задача СПС - обеспечить обнаружение нарушителя. Качество работы системы обнаружения (СО) определяется тем, что система обнаружения (СПС+ТВ) своевременно и достоверно (т.е. без пропусков и без ошибок) обнаруживает и саму угрозу и её координаты. Главными тактико-техническими характеристиками (ТТХ) СО являются $P_{обн.}$, $T_{ложн.}$.

Все понимают, что какими бы замечательными эти характеристики не были, произойдет задержание нарушителя или нет определяется эффективной работой всего комплекса СЗП, всех трех его подсистем. Следовательно, как требования к СПС, так и сам процесс проектирования СПС неправильно рассматривать в отрыве от ТТХ всей СЗП в целом.

Система защиты периметра (СЗП)



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

Значения тактико-технических характеристик создаваемых КСБ и СПС указываются в техническом задании (ТЗ) и рассматриваются как главные требования Заказчика.

Когда и как мы можем и должны контролировать выполнение этих требований?

Начинается создание системы с формирования технического задания (ТЗ), в котором отражаются все требования Заказчика и действующих нормативных документов (НД). Далее, в результате проектирования получаем проектную документацию на систему.

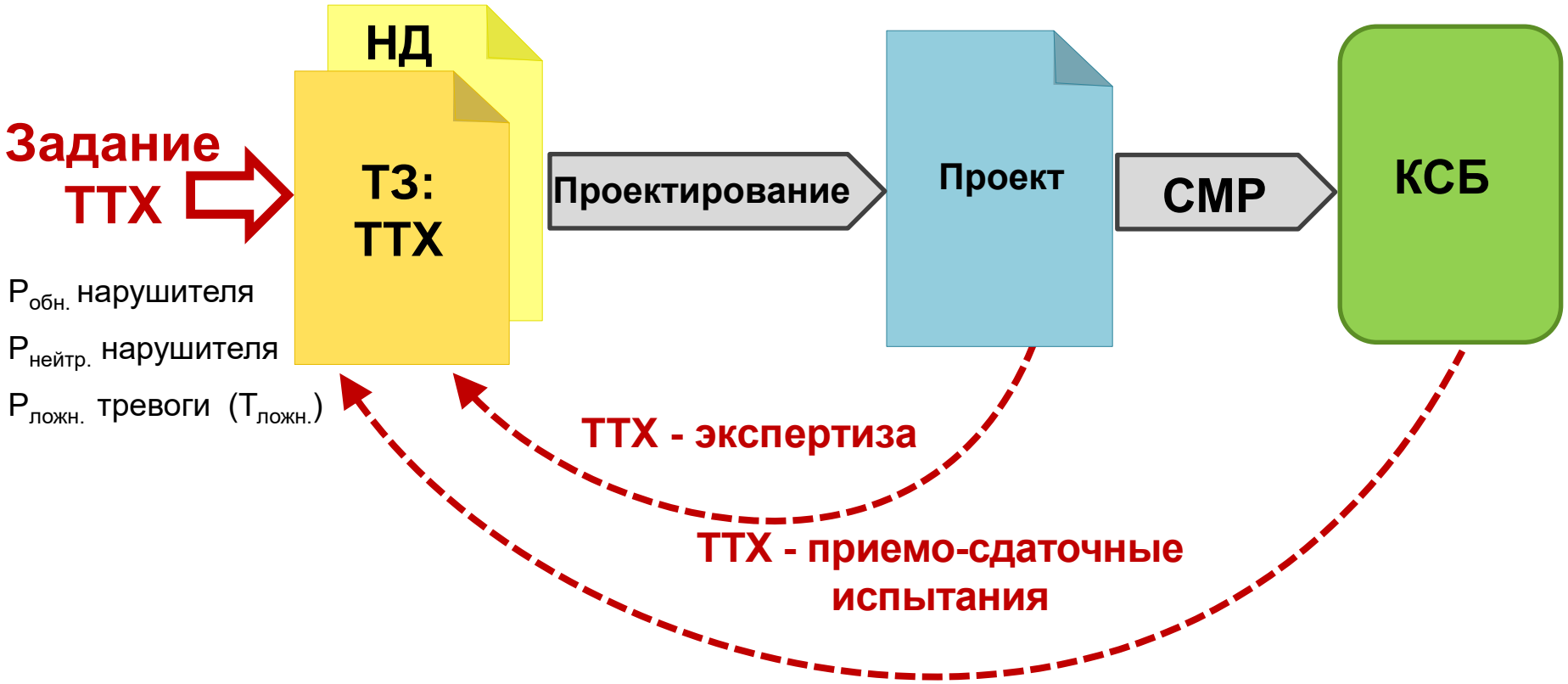
Задача №1.

Необходимо проверить, соответствует ли сделанный проект требованиям ТЗ. Если он не удовлетворяет ТЗ, то зачем в дальнейшем тратить немалые деньги на строительство КСБ или СПС? Следует корректировать проект и/или ТЗ.

Задача №2.

После выполнения строительно-монтажных работ (СМР) в ходе приемо-сдаточных испытаний (ПСИ) необходимо убедиться, что ТТХ созданной КСБ и СПС соответствуют требованиям ТЗ. Если не соответствуют, то система не принимается (не ставится на вооружение).

Система защиты периметра — всегда новый продукт



Типового проекта системы безопасности не существует.

Какими основаниями обладает разработчик ТЗ (заказчик) для задания основных ТТХ системы?

Практически никакими, кроме здравого смысла!

Поэтому ключевыми факторами принятия заказчиком решений являются цена системы и опыт.

Требования к ТТХ

1. Основания:

- Нормативная документация

ПП 458, 459, 993, 969…

$P_{обн.} > 0.95$

- Техническая документация

$P_{обн.}$: **95 … 100 %** **?**

$T_{ложн.}$: **1/мес. … 1/год** **?**

- Сертификаты, отзывы, реклама

2. Принятие решений

1. Цена
2. Опыт: «хорошо/плохо»

Как сегодня выглядит типовое ТЗ на проектирование СЗП? Из представленной таблицы достаточно понятно, что три обязательных ТТХ задаются неполно и в дальнейшем не реализуются.

Требования к системе защиты периметра

Типовое ТЗ	Реально
1. $P_{задержания}$ — требований нет $P_{задержания} = 1$ (по умолчанию)	1. $P_{задержания}$ — не интересует $P_{задержания} \neq 1$
2. $P_{обнаружения} > 0.95$	2. $P_{обнаружения}$ — неизвестна
3. $T_{ложное} >$ 1/мес. … 1/год	3. $T_{ложное} \sim$ 1/сут. … 1/мес.

Логически сделанный вывод подтверждается и результатами испытаний реально работающих систем: значения основной характеристики систем периметральной сигнализации $P_{обн}$ даже близко не соответствуют заявленным в документации и производителя, и проектировщика значениям.

Исключения составляют 13 систем, реализованных на базе «СТРАТУМ-Ограда». Более того, методами дисперсионного анализа показано, что и любая следующая система, построенная в схожих условиях на базе «СТРАТАМ-Ограда» с вероятностью 90% будет иметь ту же $P_{обн} > 0.997$.

Причина подобного положения – отсутствие на сегодня у всех (кроме компании «ПЕНТАКОН») методики и технологии обоснованно задавать и контролировать ТТХ системы.

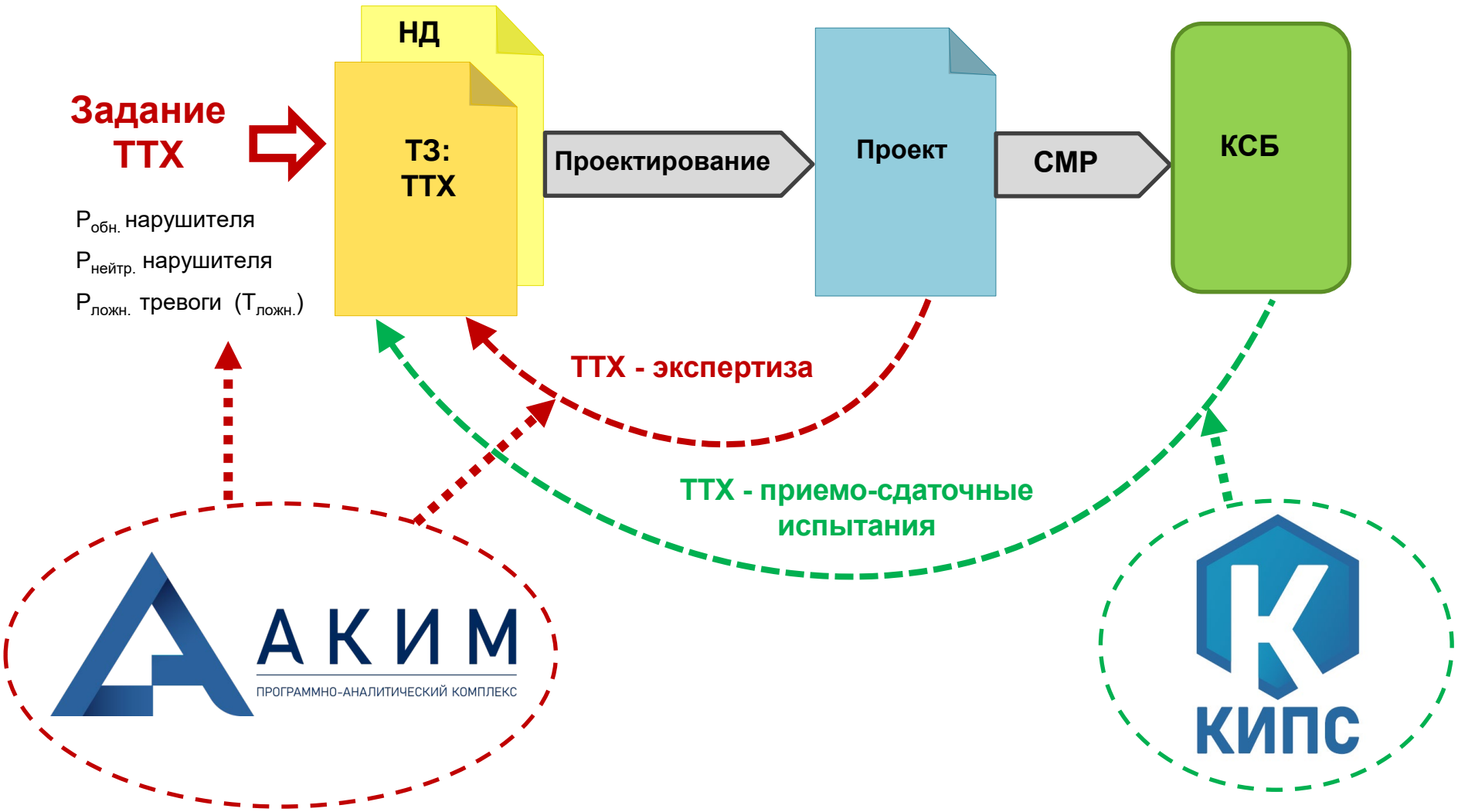
Результаты испытаний СПС

Система	Тип	$P_{обнаружения}$		Не обнаруживаются	
		Документация	Испытания		
C1	трибо	-	0.24		3 из 4 (75%)
C2 (3 испытания)	трибо	0.95	0.62		2 из 5 (40%)
C3	вибро датчики	> 0.99	0.20	**7 систем**	4 из 5 (80%)
C4	трибо	0.98	0.53		1 из 2 (50%)
C5	трибо	0.98	> 0.85 (2 канала)		1 из 6 (17%)
C6	трибо	1.0	-		?
СТРАТУМ (13 испытаний)	проводная РЛ	> 0.99	> 0.997	**13 систем**	1 из 330 (**0,3%**)

Для обоснования задания основных ТТХ системы и их последующего контроля компанией «ПЕНТАКОН» разработаны:

1. Автоматизированный комплекс имитационного моделирования «АКИМ».
2. Методика статистических приемо-сдаточных испытаний «КИПС»

Система безопасности — всегда новый продукт



Моделирование проекта создаваемой системы безопасности осуществляется с помощью диалогового автоматизированного комплекса имитационного моделирования «АКИМ», разработанного компанией «ПЕНТАКОН».

Оценка качества системы безопасности в комплексе «АКИМ» проводится путем проведения многочисленных (10^3 - 10^4) вычислительных экспериментов, имитирующих на цифровом двойнике объекта процесс реально возможных сценариев проникновения нарушителя на территорию объекта.

Назначение комплекса «АКИМ»:

1. Обоснование требований технического задания.
2. Экспертиза проектов.
3. Обоснование затрат (необходимые и достаточные).
4. Количественная оценка уязвимостей.
5. Разработка оптимальной тактики действий охраны.
6. Сертификация готовых систем.

Комплекс «АКИМ» имеет патенты Российской Федерации, ЕАЭС и Израиля, а также свидетельство о государственной регистрации.

Обоснование требований ТЗ и экспертиза

АКИМ

ПРОГРАММНО-АНАЛИТИЧЕСКИЙ КОМПЛЕКС

для проектирования, моделирования и анализа систем безопасности

Патент РФ RU 2755775 C1

Патент Израиля № 262628

Патент ЕАЭС № 043326

Свидетельство № 2023617480
О регистрации программы для ЭВМ «АКИМ»


РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023617480


РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2755775

СПОСОБ АВТОМАТИЧЕСКОГО ФОРМИРОВАНИЯ ЦИФРОВОЙ МОДЕЛИ ОХРАНЯЕМОГО ОБЪЕКТА, АНАЛИЗА СИСТЕМ БЕЗОПАСНОСТИ ОХРАНЯЕМОГО ОБЪЕКТА И ОЦЕНКИ УЯЗВИМОСТИ ОХРАНЯЕМОГО ОБЪЕКТА С УЧЕТОМ УПОМЯНУТОГО АНАЛИЗА


State of Israel
Patent Office

תעודת פטנט

CERTIFICATE OF PATENT


ЕВРАЗИЙСКАЯ ПАТЕНТНАЯ ОРГАНИЗАЦИЯ
ЕВРАЗИЙСКОЕ ПАТЕНТНОЕ ВЕДОМСТВО

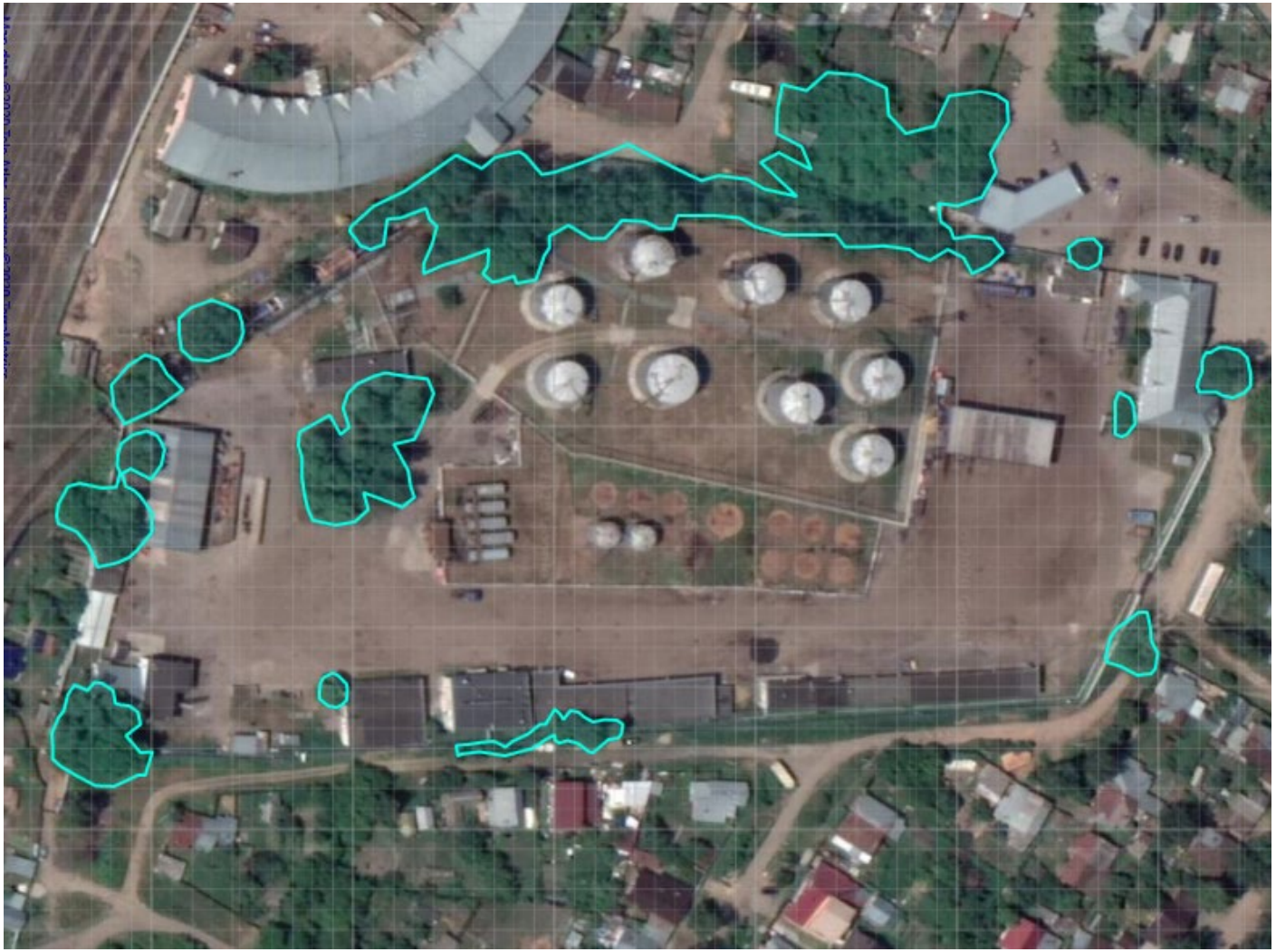
ЕВРАЗИЙСКИЙ ПАТЕНТ
НА ИЗОБРЕТЕНИЕ
№ 043326

Запись на вебинар:
https://www.cctv.ru/obuchenie-i-treningi/

Рассмотрим работу «АКИМ» на примере оценки работы СЗП некой нефтебазы.

Работы могут начаться со спутникового снимка. Относительно несложные манипуляции позволяют создать план объекта.

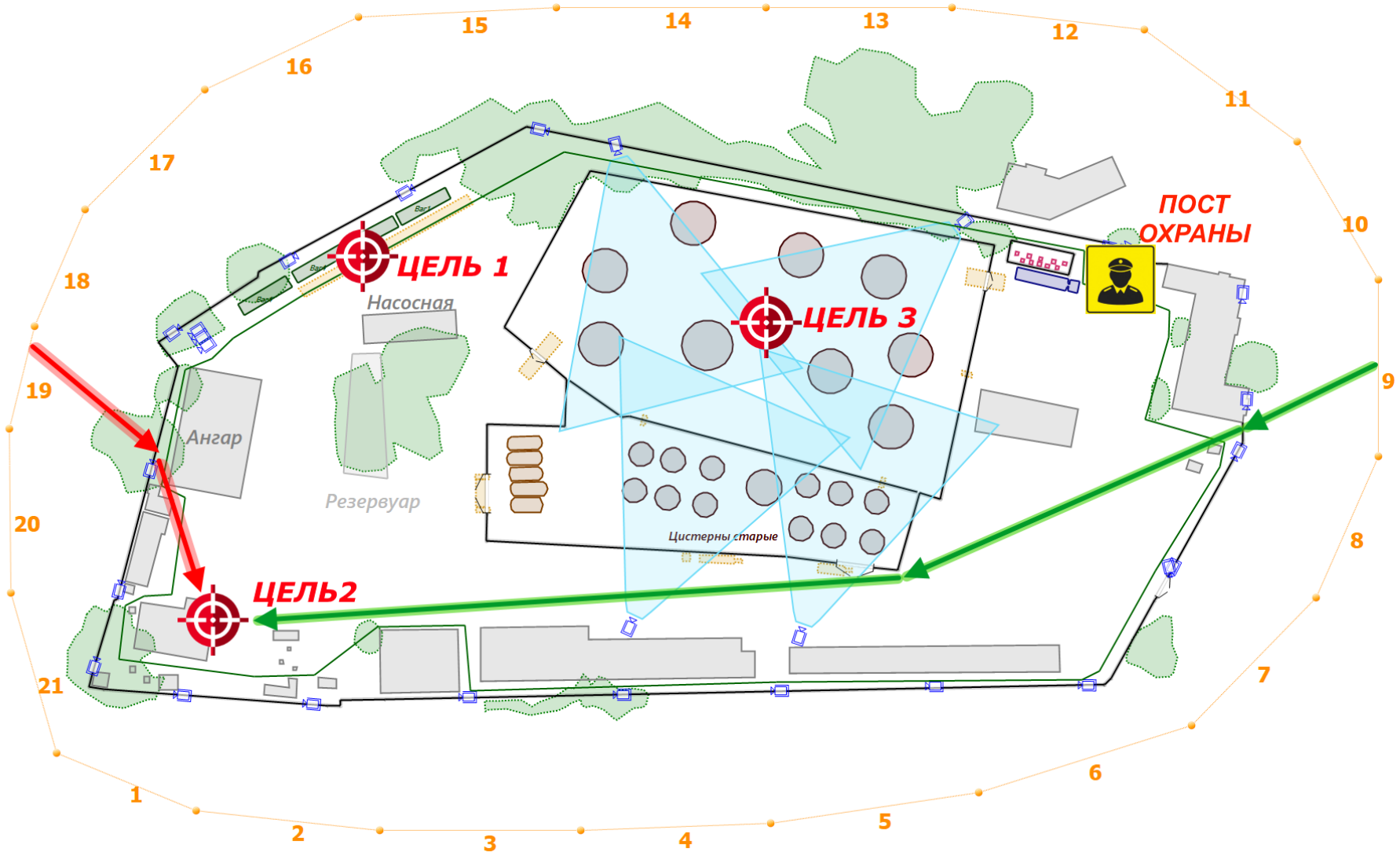
Пример моделирования: нефтебаза



Очевидно, что анализ нарушения надо производить не вообще относительно преодоления охраняемого периметра, а производить с учетом места проникновения и относительно цели внутри периметра, к которой движется нарушитель. В данном примере это цель № 2. К слову, кто-то сегодня может учитывать при проектировании такие подробности, как разные цели нарушителя? Важно заметить, что успех/неуспех действий нарушителя и его нейтрализация зависит и от того, каким путем движется нарушитель, и от расположения службы охраны, и от тактики ее действий.

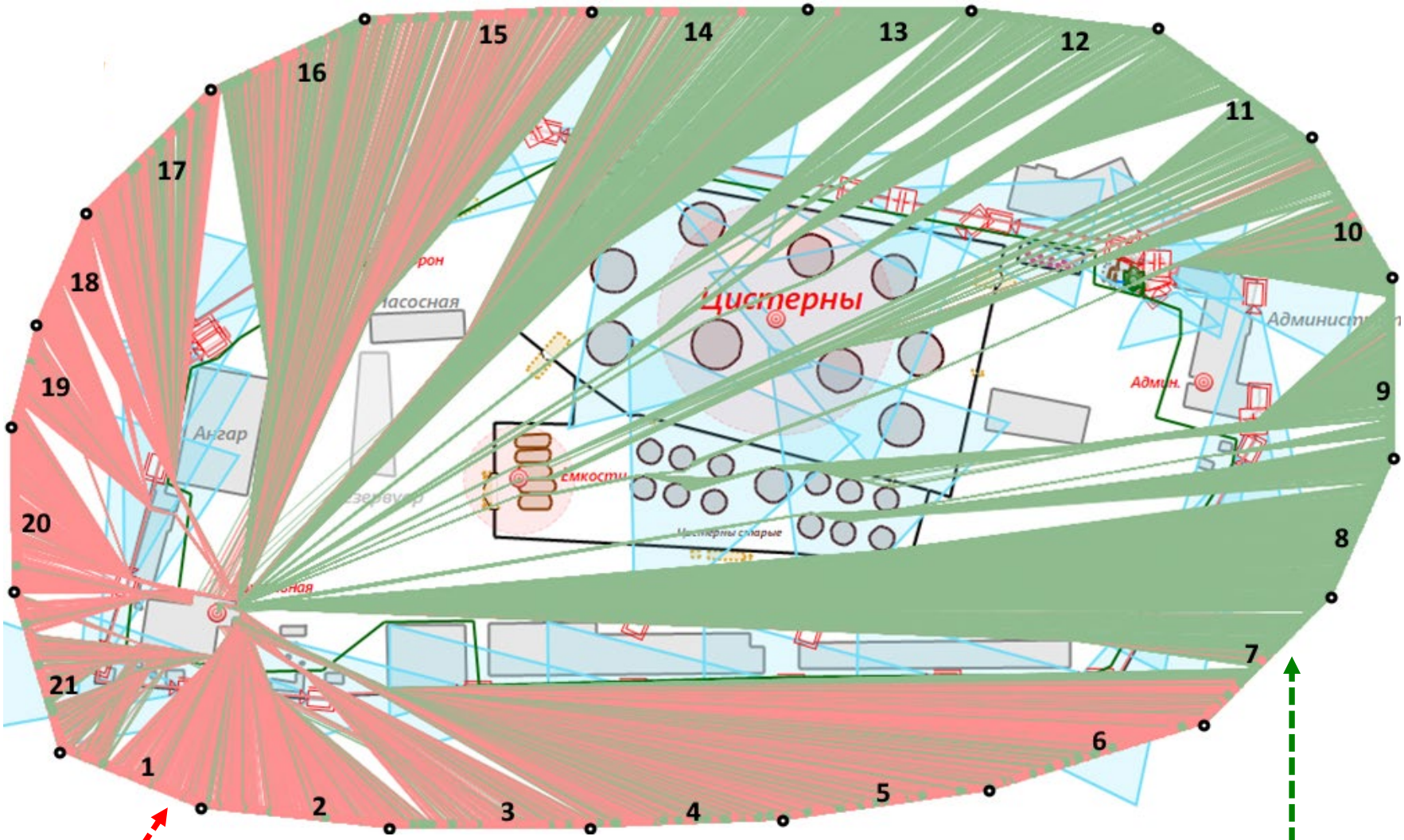
На следующем слайде приведены результаты моделирования одного из вариантов СЗП этого объекта при проникновении нарушителя 10^4 раз к цели № 2.

Пример моделирования: план объекта



На слайде показаны все возможные варианты движения нарушителя к цели №2 (10^4 попыток). Видно, что при проникновении на объект (к цели №2) с участков периметра 1-6, 17-21 служба охраны не успевает задержать нарушителя.

Пример моделирования: траектории атак



Нарушитель дошел до цели

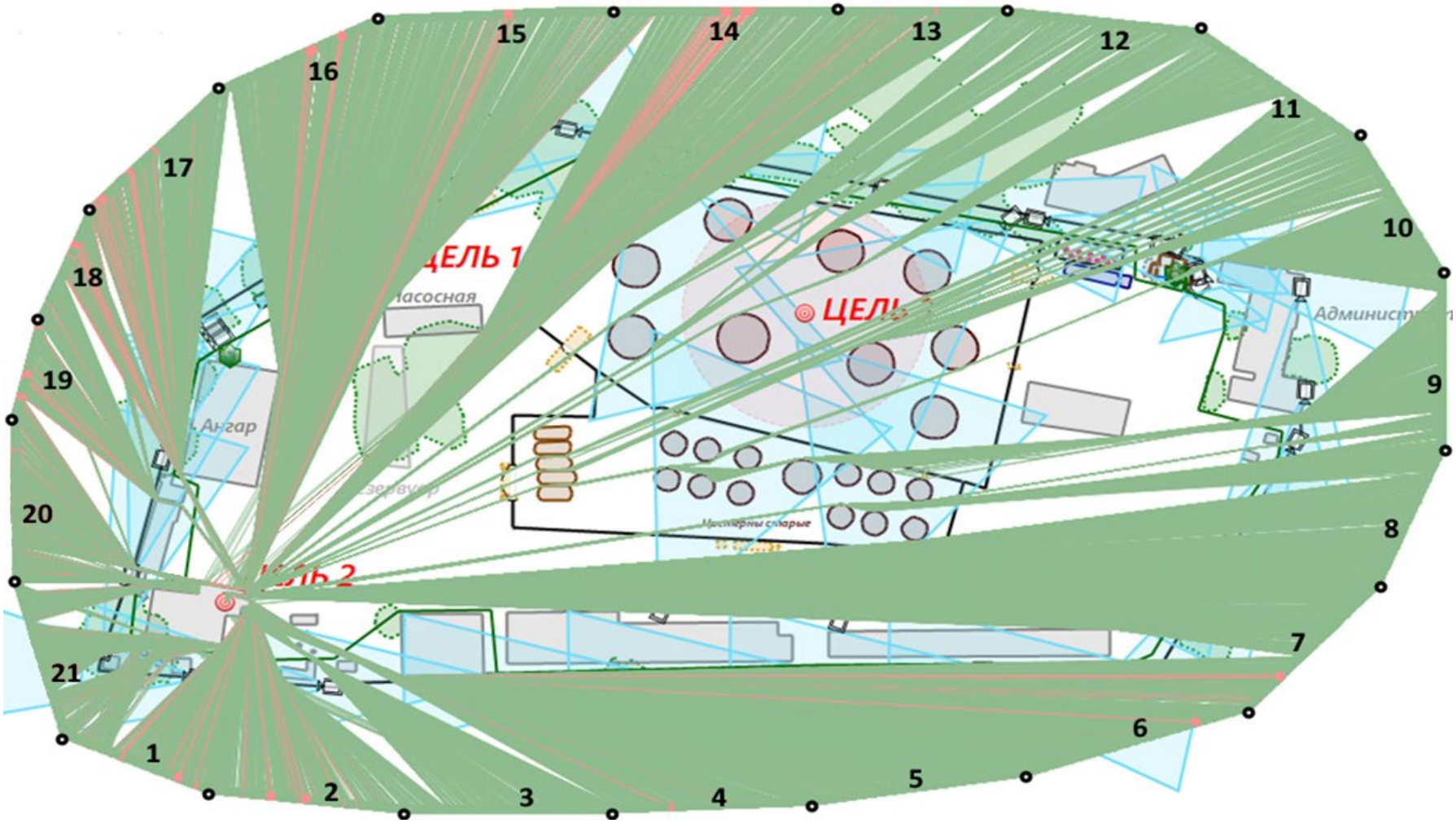
Нарушитель был нейтрализован

Усовершенствуем систему (+1% к стоимости): введем в систему еще один пост охраны.

Пример моделирования: новый пост охраны

По результатам очередных 10^4 испытаний положение дел кардинально улучшилось.

Пример моделирования: траектории атак после



Полученные результаты моделирования могут быть представлены и в виде гистограмм.

Наглядно показано:

- даже при 100% обнаружении существуют участки периметра, при проникновении через которые нарушитель может быть нейтрализован всего лишь с вероятностью 2-3%;
- дополнительные (1%) затраты способны кардинально улучшить качество работы СЗП;
- работа системы сигнализации и службы охраны должны рассматриваться совместно, в едином комплексе, называемом системой защиты периметра (СЗП).

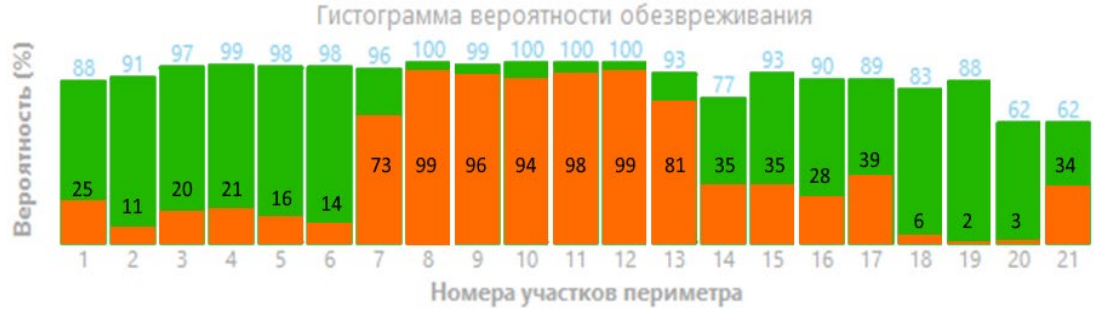
Пример моделирования: результаты 10^4 попыток

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%

«АКИМ» позволяет моделировать ситуации и находить оптимальные решения по противодействию другим типам нарушителя, например, БПЛА.

Борьба с БПЛА: моделирование

Система обнаружения **СПС + ТВ**

Ограждение **ИТС**

Система задержания **Патруль**

Нарушитель

Нейтрализация

Система обнаружения БПЛА

Система подавления БПЛА

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

Завершающим этапом создания системы безопасности является проведение статистических приемо-сдаточных испытаний (ПСИ). Статистических потому, что основные ТТХ системы начинаются со слова «вероятность».

Сегодня принято проводить только ПСИ с целью проверки функционирования оборудования. Фрагментарно (обычно в инициативном порядке) собирается небольшая статистика для оценки $P_{обн.}$, $P_{ложн.}$. Степень достоверности этих оценок крайне низка.

Сегодня оценки качества работы СПС формулируются на уровне «хорошо»/«плохо» («срабатывает»/«не срабатывает»).

Для корректного решения этих задач необходимы научно-обоснованные методики испытаний. Компания «ПЕНТАКОН» разработала и предлагает такие Методики «КИПС».

Методики основаны на действующих ГОСТах и запатентованы. Они определяют порядок проведения статистических испытаний сложных систем по методу контрольных испытаний.

По сравнению с методикой доверительных интервалов объем и продолжительность необходимых экспериментов сокращается в разы и даже на порядок. При этом параллельно также вычисляются и точечные оценки параметров и их доверительные интервалы.

Проведение статистических приемо-сдаточных испытаний (ПСИ)

МЕТОДИКИ КИПС

На базе ГОСТ Р 27.403-2009 ГОСТ 27.402-95

Основные этапы

КИПС

- Обоснование выбора участка для ПСИ
- Обоснование выбора способа преодоления
- Составление плана контрольных испытаний
- Проведение испытаний

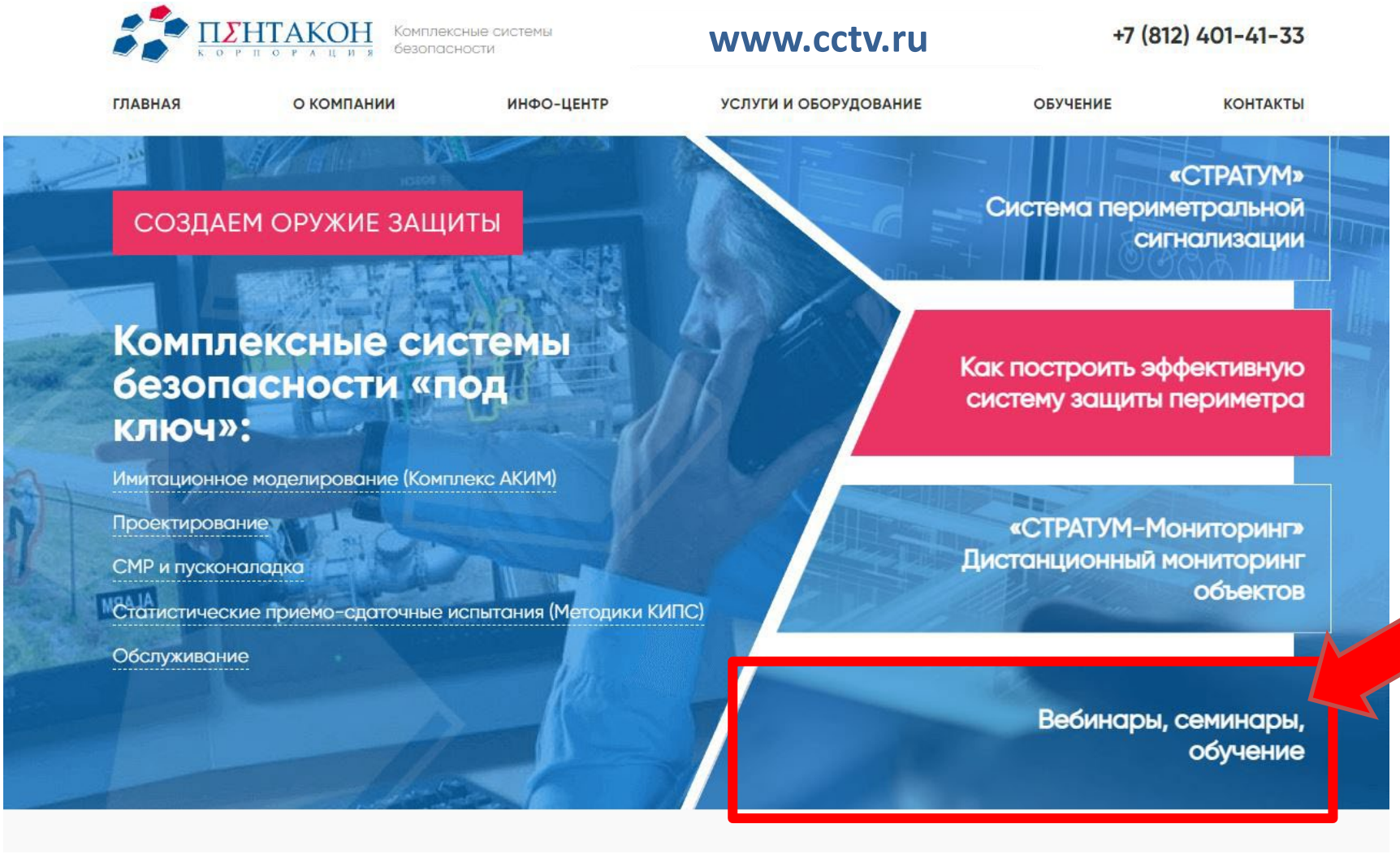
Патент РФ RU 2 768 859 C1

Свидетельство № 2020618224
О регистрации программы для ЭВМ «Программный комплекс АКИМ-КИПС»

Более подробную информацию по всем системам и методикам компании «ПЕНТАКОН» можно получить на сайте.

Приглашаю на наши регулярные вебинары.

Приглашение на регулярные вебинары



Заключение

СПАСИБО ЗА ВНИМАНИЕ !

Президент компании ПЕНТАКОН
к.т.н., доцент,
Крылов Виктор Михайлович

Krylov@cctv.ru
www.cctv.ru

ПЕНТАКОН
КОРПОРАЦИЯ

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

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