

УДК 519.72

**ЧЕМ ИЗМЕРИТЬ ЭФФЕКТИВНОСТЬ:  
МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ  
ФИЗИЧЕСКОЙ ЗАЩИТЫ ОХРАНЯЕМЫХ ОБЪЕКТОВ УИС**

**Е.Г. Царькова** главный научный сотрудник ФКУ НИИИТ  
ФСИН России, кандидат физико-математических наук,  
докторант ФГБОУ ВО «Тверской государственный  
технический университет»

---

**Аннотация**

В работе анализируются методы оценки эффективности инженерно-технических средств охраны и надзора, используемых в учреждениях УИС. Рассматриваются перспективные направления автоматизации деятельности сотрудников уголовно-исполнительной системы Российской Федерации в области оценки эффективности охранных систем. Приводится описание возможностей специализированного программного обеспечения для решения исследуемого класса задач. Рассматриваются возможности базы данных технических средств охраны, а также перспективы ее практического применения в УИС при анализе инженерно-технической защищенности объекта.

**Ключевые слова**

эффективность, оценка эффективности, системы физической защиты, охраняемый объект уголовно-исполнительной системы

---

Учитывая нарастающую нестабильность в мировой политике, экономике и обществе, в настоящее время решение задач предупреждения и обнаружения противоправных действий на объектах охраны и надзора уголовно-исполнительной системы Российской Федерации приобретает все большую актуальность.

Для успешного противодействия противоправным действиям нарушителя недостаточно применения типовых решений построения системы физической защиты (СФЗ), предлагаемых производителями. Поскольку фактически каждый объект охраны УИС уникален, при создании конкретной СФЗ необходимо учитывать как факторы, напрямую влияющие на проектные решения (архитектурные особенности территории, режим работы, модель нарушителей, частные задачи, которые должна решить СФЗ, сведения о численности персонала и т.п.), так и неочевидные (топология окружающей территории, криминогенная внешняя и внутренняя обстановка, погодные условия, флора и фауна местности и множество других). При проектировании СФЗ зачастую рождается несколько решений, и выбор наиболее подходящего основывается на экспертном мнении, которое не всегда является объективно верным.

---

Создание системы физической защиты объекта предполагает анализ эффективности и уязвимости СФЗ. В свою очередь, сложность современных СФЗ, а также многообразие моделей нарушителей и способов их противоправных действий влечет необходимость применения средств автоматизации процессов моделирования таких систем. В основе различных методов анализа эффективности СФЗ лежат данные экспертных оценок основных параметров, и, следовательно, эти методы обладают высокой степенью субъективности. Для их реализации требуются трудоемкие экспериментальные исследования. Кроме того, их сложно использовать в задачах математического моделирования.

Таким образом, для специалистов в области обеспечения безопасности актуальными являются вопросы повышения точности анализа эффективности СФЗ охраняемых объектов УИС, а также разработки методов анализа эффективности СФЗ, применимых, в том числе, и к задачам компьютерного моделирования действий нарушителя с учетом вероятностного характера различных процессов (действий нарушителя при преодолении физических барьеров, вероятности его обнаружения и т.п.) [2].

Анализ практики и особенностей использования критериев эффективности в регулировании и обеспечении физической защиты охраняемых объектов УИС показывает, что оценка эффективности СФЗ является сложным инструментом, использование которого требует разработки и освоения сотрудниками, обеспечивающими безопасность, специальных подходов, методов, моделей и методик.

Безусловно, полностью автоматизировать процесс оценки эффективности СФЗ и исключить человеческий фактор невозможно, однако задача существенного его упрощения и систематизации решаема. В связи с этим необходима разработка решения, учитывающего ведомственную специфику и позволяющего получить обоснованную численную оценку вероятности обнаружения неблагоприятного воздействия на защищаемый объект и его своевременного пресечения. Это дает возможность провести оптимизацию по основным критериям при организации (проектировании) СФЗ, среди которых могут быть выделены: максимальный уровень защиты при заданных затратах и заданный уровень защиты при минимальных затратах.

Несмотря на большое количество публикаций в области систем физической защиты, ряд вопросов создания и оценки эффективности СФЗ охраняемых объектов УИС остаются недостаточно исследованным. Поэтому задача разработки моделей и методов анализа эффективности СФЗ охраняемого объекта УИС, а также оценки вероятности обнаружения нарушителя и своевременного пресечения противоправного действия на объекте охраны является значимой.

Целью данного исследования является:

1. Выполнение сравнительного анализа применяемых методов оценки эффективности СФЗ и формулировка основных требований к разрабатываемому методу анализа эффективности СФЗ охраняемого объекта УИС;

2. Формулировка критериев оценки эффективности инженерно-технических средств СФЗ и систем этих средств;

3. Обоснование методики анализа эффективности инженерно-технических средств СФЗ объектов охраны и надзора УИС.

Под эффективностью технической системы, как правило, понимают ее приспособленность к выполнению своей целевой функции. Государственный стандарт [1] определяет эффективность автоматизированной системы как «свойство, характеризующее степень достижения целей, поставленных при создании системы». В частности, эффективность СФЗ можно трактовать как способность системы противостоять несанкционированным действиям нарушителя в рамках проектной угрозы.

При этом различают два различных оттенка понятия «эффективность»:

1. *Эффективность (efficiency)* – соотношение между достигнутыми результатами и ресурсами, которые были затрачены;

2. *Результативность (effectiveness)* – степень достижения результатов, которые запланированы.

При всей важности экономической эффективности для охраняемого объекта УИС будет логичнее понимать под эффективностью СФЗ именно результативную эффективность, а эффективность в смысле экономичности выделять в группу комплексных показателей вида «эффективность – стоимость».

Оценка эффективности – это процедура (исследование), проводимая, как правило, в ходе анализа уязвимости и направленная на определение количественных и/или качественных показателей эффективности, выявление критических элементов СФЗ, а также нахождение интегрального показателя эффективности системы в целом. При системном подходе к созданию СФЗ результаты оценки эффективности выступают в качестве исходных данных для этапа рабочего проектирования охранной системы [4,5].

На основании проведенного обзора методов оценки эффективности СФЗ можно выделить следующие:

**1. Детерминистический подход** к оценке эффективности СФЗ:

- позволяет судить о степени выполнения требований руководящих документов по принципу: «выполнено-не выполнено». Метод прост в применении, не содержит сложных математических расчетов, что позволяет применять его без использования дополнительных программных пакетов. При этом используется система факторов состояния (ФС), которые определяют организацию и обеспечение физической защиты в соответствии с требованиями нормативных документов.

Различают: ФС организационных мероприятий (группа а), ФС инженерно-технических средств охраны (группа б), ФС действий подразделений охраны (группа с).

Эксперт выбирает некоторое количество ФС по группам  $a, b, c$  соответственно. Каждому ФС каждый эксперт назначает определенный «вес», а также дает оценку степени реального состояния ФС ( $d = 1, 2, 3$ ). Далее определяется среднее значение показателя реального состояния каждого ФС по всем экспертам (рис.1,2). Возможность определения показателя состояния как всей системы в целом, так и ее составных частей позволяет выявлять ее «слабые звенья».

Показатель состояния:	Формула для его оценки
— организационных мероприятий	$N_1 = \frac{\sum_{i=1}^k a_i d_i}{d_m k a_m}$
— инженерно-технических средств	$N_2 = \frac{\sum_{i=1}^l b_i d_i}{d_m l b_m}$
— действий подразделений охраны	$N_3 = \frac{\sum_{i=1}^m c_i d_i}{d_m m c_m}$
$k$ — число ФС в организационных мероприятиях; $l$ — число ФС в инженерно-технических средствах ФС; $m$ — число ФС в действиях подразделений охраны; $d_m$ — максимально возможное значение показателя реального состояния ФС ( $d_m = 3$ ); $a_m, b_m, c_m$ — максимально возможные значения весов ФС в группе ФС (5, 7, 10 соответственно).	

Рисунок 1 – Оценки показателей факторов состояния

Значение показателя состояния N:	Соответствие ФЗ требованиям
$N \leq 0,05$	ФЗ не обеспечивается
$0,05 < N < 0,07$	Имеет значительные отступления от требований норм и правил, требующие использования компенсирующих мероприятий
$0,07 < N < 0,1$	ФЗ имеет отдельные отступления от требований норм и правил
$N \geq 0,1$	ФЗ в основном соответствует требованиям норм и правил

Рисунок 2 – Интерпретация результатов оценки состояния физической защиты (ФЗ)

Поскольку метод является полностью экспертным, достоверность оценки сильно зависит от компетентности экспертов. Также на основании детерминистического подхода нельзя оценить правильность размещения и настройки инженерно-технических средств защиты, применения сил охраны, средств обнаружения и т.п. Кроме того, руководящие документы со временем могут терять актуальность, а вступление в силу обновленного документа также требует пересмотра критериев оценки, т.е. факторов защиты.

Реальные тактико-технические характеристики СФЗ в данном методе оценки не используются. А поэтому детерминистический подход целесообразно применять лишь как предварительный этап оценки или в качестве профилактических мероприятий. Результаты оценки таким способом могут послужить предпосылкой для детального анализа степени эффективности системы и дальнейшей модернизации.

Таким образом, к недостаткам данного метода можно отнести отсутствие учета реальных характеристик СФЗ; высокую зависимость достоверности оценки от компетентности экспертов и их осведомленности об объекте, угрозах, СФЗ и т.п.; узкую специфику метода; невозможность оценки правильности размещения и настройки инженерно-технических средств защиты, применения сил охраны, средств обнаружения и т.п.; зависимость исходных данных (факторов защиты) от действующих нормативных документов.

**2. Метод логико-вероятностного моделирования** позволяет получить вполне обоснованный количественный показатель эффективности. Кроме того, он позволяет построить наглядную структуру функционирования СФЗ с указанием всех подсистем, выявить «слабые места» системы и оценить вклад каждого из них в степень риска. Вычисляемые в ходе применения метода значения вероятностной функции

показывают, какова вероятность преодоления нарушителем системы охраны объекта необнаруженным и не дают оценки вероятности его задержания. При этом структура СФЗ описывается с применением функций алгебры логики, а количественная оценка проводится с помощью теории вероятности.

В ходе процедуры оценки составляется сценарий развития опасности, представляющий собой логико-вероятностную модель функционирования СФЗ. Сценарий представляется в виде графа и содержит события трех видов: иницирующие, промежуточные, конечное. Иницирующие события описывают воздействия нарушителя на систему (преодоление периметра объекта, имитация процедуры идентификации на КПП и др.). Промежуточные события получаются путем логической комбинации двух или более событий (конъюнкция, дизъюнкция событий и др.). Конечное событие описывает определенное опасное состояние системы (например, проникновение нарушителя к цели акции раньше группы караула) (рисунок 3).

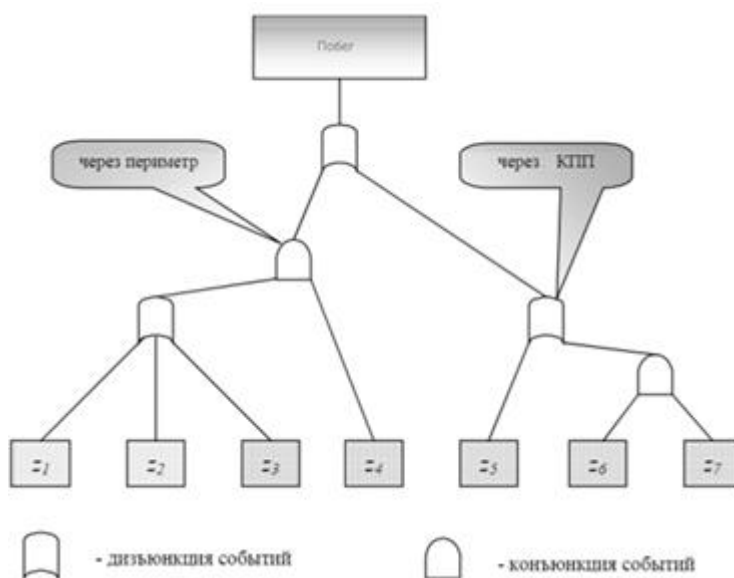


Рисунок 3 – Схема логико-вероятностного метода

Далее составляется функция опасности системы, аргументами которой являются иницирующие события, а значением — конечное (опасное) событие. Затем ищется значение полученной вероятностной функции в предположении реализации опасного события, определяющее степень риска, присутствующего в системе.

Можно выделить ряд недостатков метода: отсутствие учета временных характеристик процесса преодоления физических барьеров; сложность расчетов вручную при работе со сложными объектами или сложными сценариями нарушений в связи с большим количеством трудоемких математических преобразований; трудности с отображением последовательных действий на схеме для сложных объектов; проблема исходных данных (вероятностных характеристик СФЗ и нарушителя).

3. **Метод анализа иерархий** (МАИ) позволяет построить содержательную модель нарушителя, проанализировать возможные угрозы, оценить эффективность элементов СФЗ с учетом модели нарушителя и угроз [6-8]. С помощью МАИ можно, например, на этапе проектирования или модернизации системы рассмотреть возможные альтернативы построения СФЗ (рисунок 4).

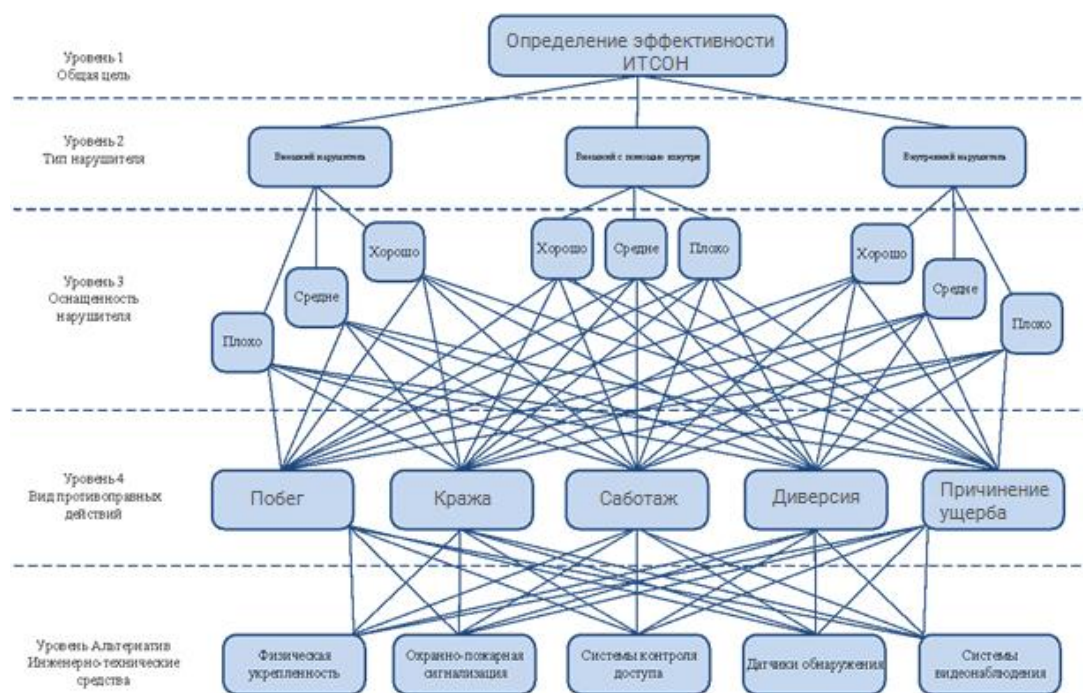


Рисунок 4 - Схема метода анализа иерархий

Явным недостатком МАИ является то, что с его помощью нельзя провести количественную оценку эффективности конкретной СФЗ, а можно лишь качественно сравнить СФЗ нескольких объектов между собой. Это накладывает определенные ограничения на использование метода.

Полученные в ходе метода количественные критерии по уязвимости не являются абсолютными, а представляют лишь количественно выраженные предпочтения эксперта. Поскольку количественный критерий по уязвимости – относительная величина, зависящая от количества объектов, представленных к сравнению, при изменении количества объектов потребуется пересмотр критериев.

Как и в случае детерминистического подхода, показатель эффективности, полученный в результате МАИ, не отражает реальные характеристики СФЗ и нарушителя. В литературе отмечают также другие недостатки математического аппарата МАИ. В частности, замечают, что шкалы, в которых осуществляется оценивание предпочтений альтернатив по каждому из критериев, являются шкалами отношений, не связанными

ни друг с другом, ни с приоритетами критериев. В результате МАИ работает не всегда корректно при определенных наборах входных данных.

Таким образом, к недостаткам данного метода можно отнести отсутствие учета реальных характеристик СФЗ; относительность величины получаемого показателя эффективности системы; сильную зависимость качества оценки от квалификации аналитиков (экспертов); недостатки математического аппарата при работе с некоторыми сценариями.

**4. Метод вероятностно-временного анализа**, основываясь на реальных характеристиках СФЗ, дает обоснованную оценку эффективности. Эффективность физической защиты рассматривается здесь как вероятностная величина - вероятность того, что силы охраны, действующие по сигналам тревоги технических средств охраны, успеют пресечь акцию нарушителя (рис. 5).

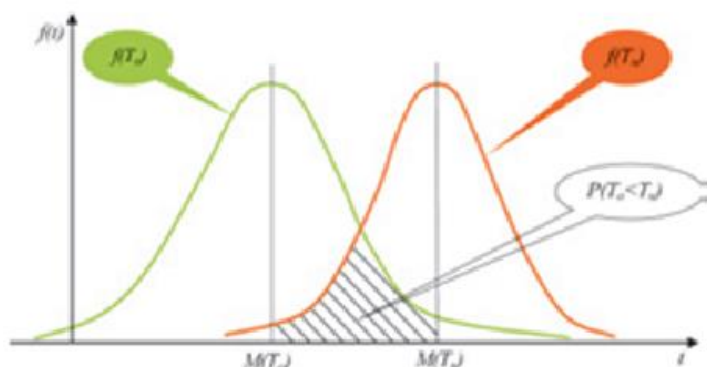


Рисунок 5 – Графическая интерпретация вероятности своевременного пресечения действий нарушителя

Для расчета данной вероятности анализируются маршруты движения нарушителей и сил охраны для каждой из целей, определенных на этапе анализа уязвимости. Оцениваются времена движения, относящиеся к различным этапам их действий. Для нарушителя это могут быть время преодоления физических барьеров, время движения по территории объекта, время акции и т.д., для охраны — время сборов, время движения, время осмотра сработавшего участка периметра и др.

Степень точности оценки зависит от типа исходных данных (качественный или количественный анализ). В ходе метода могут быть выявлены критические элементы СФЗ, такие, как критическая точка обнаружения, критический маршрут нарушителя. На основании этих данных можно определить пути улучшения системы, например, установку дополнительных извещателей с заданными техническими характеристиками для повышения вероятности обнаружения, установку дополнительных препятствий, повышающих суммарную вероятность обнаружения, корректировку тактики сил охраны и т.д.

Для данного метода также можно выделить ряд недостатков, таких, как проблема исходных данных; трудоемкость осуществления расчетов вручную для сложных объектов с множеством вероятных маршрутов

перемещения нарушителя; необходимость совершенствования метода расчета с учетом угрозы внутреннего нарушителя и ряд других. Тем не менее, данный метод является наиболее распространенным при оценке физической защищенности охраняемых объектов.

Таким образом, на основании анализа недостатков существующих моделей могут быть сформулированы требования к применяемому в УИС методу оценки:

1. Метод должен быть применим, по возможности, ко всем типам охраняемых объектов и быть инвариантным к характеру и способу реализации угроз;

2. Метод должен давать обоснованный показатель эффективности, отражающий реальные характеристики СФЗ объекта;

3. Необходимо в максимально возможной степени учитывать временные и вероятностные характеристики СФЗ, т.е. время реагирования и вероятности обнаружения, а также временные и вероятностные характеристики акции нарушителя, т.е. времена преодоления барьеров и вероятности выбора нарушителем того или иного маршрута;

4. Необходим учет зависимости вероятности обнаружения от квалификации нарушителя;

5. Должна быть предоставлена возможность создания компьютерной модели на основании разрабатываемого метода для случая сложности математических расчетов;

6. Должна быть обеспечена гибкость метода по отношению к типу исходных и других данных, т.е. возможность определения данных как экспериментальным путем, так и на основании экспертных оценок.

Метод оценки эффективности СФЗ объектов охраны УИС, таким образом, строится на моделировании цепочки событий: «обнаружение вероятного нарушителя» – «передача информации охране и ее оценка» – «принятие решения по цели ложная/истинная» – «пресечение действий нарушителя».

Так, показатель эффективности системы охраны периметра (СОП) в этом случае определяется через вероятность пресечения  $P_{пр}$  опасного события – вероятности того, что время реакции сил реагирования  $t_{рг}$  ( $t_{рг}$  – величина, зависящая от оперативности действий группы караула), окажется меньше плотности ИТСОН ( $\rho_{итсон}$ ) – суммы значений времени преодоления элементов системы защиты, расположенных после первого рубежа обнаружения. Тогда об эффективности системы защиты верно будет говорить, если обеспечена своевременность реагирования системы охраны на происшествие.

Для системы охраны периметра исправительного учреждения эффективность ( $\Phi$ ) будет определяться эффективностью функционирования её отдельных участков  $\Phi_i, i = \overline{1, m}$ :

$$\Phi = \sum_{i=1}^m k_i \Phi_i = \sum_{i=1}^m \frac{N_i}{N} \Phi_i,$$

где  $m$  – количество участков периметра,  $k_i$  – коэффициент, определяющий относительное количество попыток преодоления периметра на данном участке;  $N_i$  – количество попыток преодоления периметра на  $i$ -м участке;  $N$  – общее количество попыток преодоления периметра.

Каждый участок периметра имеет определенный набор элементов, который характеризуется различными свойствами: надежностью элементов комплекса инженерно-технических средств охраны; вероятностью обнаружения нарушителя; способностью задержания нарушителя на заданное время; способностью оповещения о попытке нарушения; подготовленностью личного состава.

Таким образом, система охраны периметра и ее отдельные элементы могут быть охарактеризованы частными показателями эффективности:

Таблица 1 - Частные показатели эффективности

$K_{исон}$	- коэффициент готовности инженерных средств охраны;
$K_{ссыон}$	- коэффициент готовности аппаратуры системы сбора и обработки информации;
<i>коэффициент готовности линий связи:</i>	
$K_{да}$	- «датчики–станционная аппаратура»;
$K_{ан}$	- «станционная аппаратура – группа караула»;
<i>вероятность обнаружения нарушителя техническими средствами при попытке преодолеть периметр:</i>	
$P_{до1}$	- путем перелаза через ограждение;
$P_{до2}$	- путем разрушения полотна ограждения;
$P_{до3}$	- путем подкопа;
<i>вероятности попыток совершения нарушения различными способами:</i>	
<i>(вероятности <math>\gamma_i, i = \overline{1,3}</math>, определяются отношением числа попыток несанкционированного преодоления каждым из указанных способов к общему числу попыток):</i>	
$\gamma_1$	- путем перелаза через ограждение;
$\gamma_2$	- путем разрушения полотна ограждения;
$\gamma_3$	- путем подкопа;
$t_3$	- минимальное значение времени задержания нарушителя инженерными средствами охраны (время, необходимое нарушителю для преодоления инженерных заграждений, установленных на пути его движения);
$t_H$	- максимальное значение времени движения группы караула до места нарушения;
$P_{пр}$	- вероятность предотвращения нарушений силами охраны.

Тогда для оценки эффективности СОП на отдельном участке справедливо соотношение [2]:

$$\Phi_i = P_{\text{ПР}} \cdot K_{\text{ССиОИ}} \cdot \sum_{j=1}^3 (\gamma_i \cdot P_{\text{ДО}_j}) \cdot K_{\text{ДА}} \cdot K_{\text{АН}} \cdot K_{\text{ИСОИ}}$$

Анализ полученного выражения позволяет сделать вывод о том, что СОП будет эффективной при условии достоверного обнаружении нарушителя техническими средствами ( $P_{\text{ДО}_j} \rightarrow 1$ ), оповещении сил охраны техническими средствами (т.е. при работоспособном состоянии системы сбора и обработки информации, а также линий связи ( $K_{\text{ССиОИ}} \rightarrow 1$ ;  $K_{\text{ДА}} \rightarrow 1$ ;  $K_{\text{АН}} \rightarrow 1$ ), и при работоспособном состоянии инженерных средств охраны ( $K_{\text{ИСОИ}} \rightarrow 1$ ). При этом инженерные средства охраны должны обеспечивать задержание нарушителя на время  $t_3$ , большее времени, необходимого резервной группе караула для предотвращения нарушения ( $t_{\text{П}}$ ). Несоблюдение этого условия приводит к существенному снижению эффективности СОП ( $P_{\text{ПР}} \rightarrow 0$ ). Таким образом, инженерно-технические средства охраны, установленные на периметре объекта, должны обеспечивать высокую вероятность обнаружения, подачи сигнала тревоги и необходимое время задержания нарушителя.

Для объектов, обладающих сложной конфигурацией охраняемых зон, маршрутов движения нарушителей и множеством целей противоправных действий, оценка эффективности может быть выполнена, как правило, только с использованием специализированных программных комплексов [8].

Создание специализированных программных средств с учетом ведомственной специфики УИС сможет обеспечить реализацию метода математического моделирования приведенной выше цепочки событий. При этом за основу метода оценки эффективности системы защиты периметра охраняемого объекта УИС вполне обоснованно может быть принято уравнивание характеристических времен движения нарушителя и сил охраны.

Для описания инженерной укреплённости объекта должна быть создана база данных инженерных средств охраны с описанием их количественных и качественных характеристик (рисунок 6).

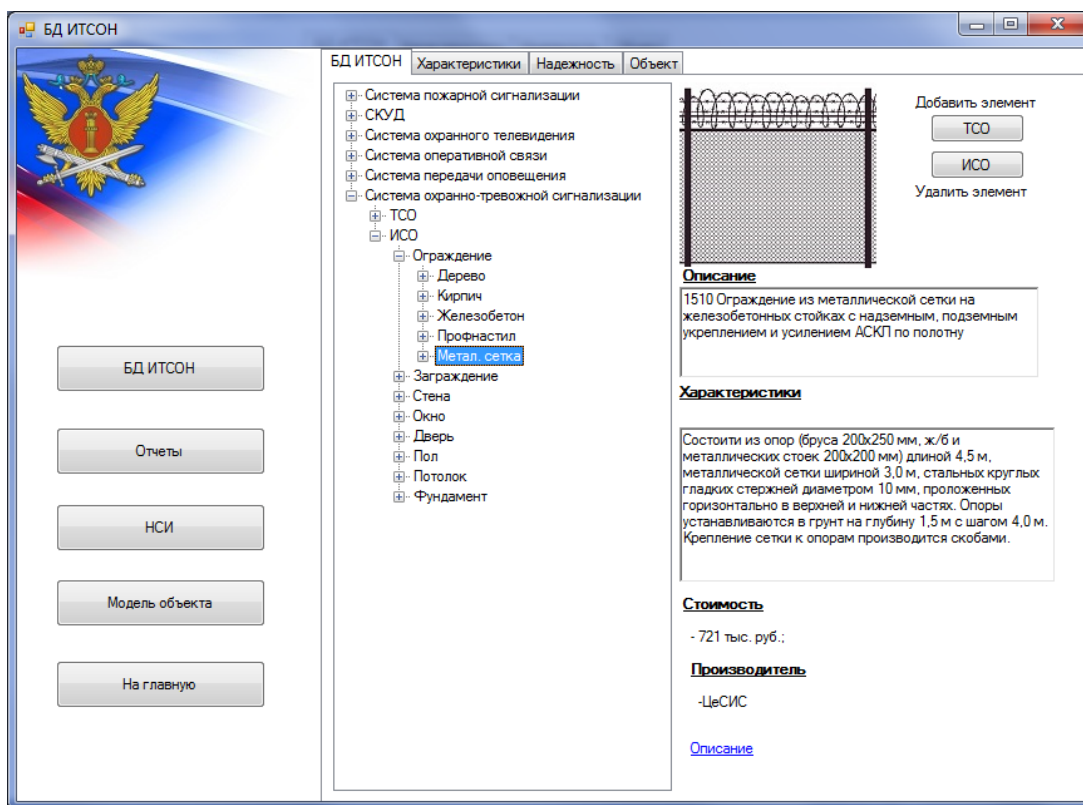


Рисунок 6 - Интерфейс формирования базы данных инженерных средств охраны

Для описания технической оснащённости объекта требуется создание базы данных технических средств охраны с описанием их тактико-технических характеристик (рисунок 7).

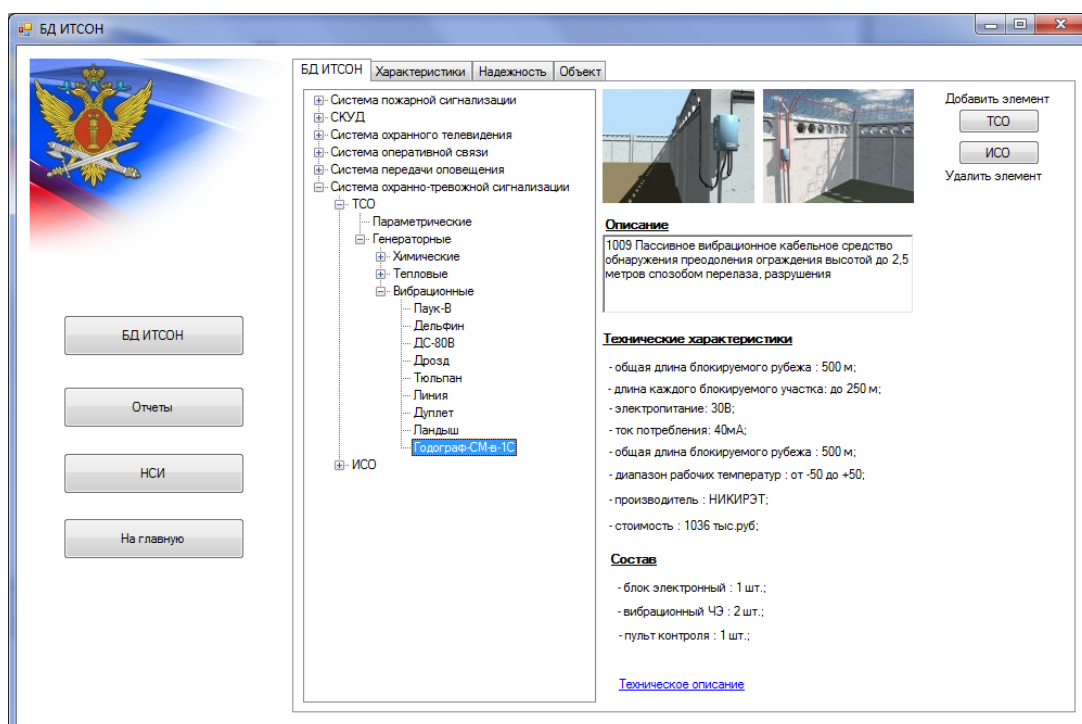


Рисунок 7 - Интерфейс формирования базы данных технических средств охраны

Также должна быть создана подсистема моделирования взаимодействия нарушителя и системы защиты с использованием схемы объекта, предназначенная для расчета вероятностно-временных характеристики преодоления нарушителем системы охраны и проверки выполнения условия пресечения группой караула опасного события за время, меньшее, чем время движения нарушителя (рисунок 8).

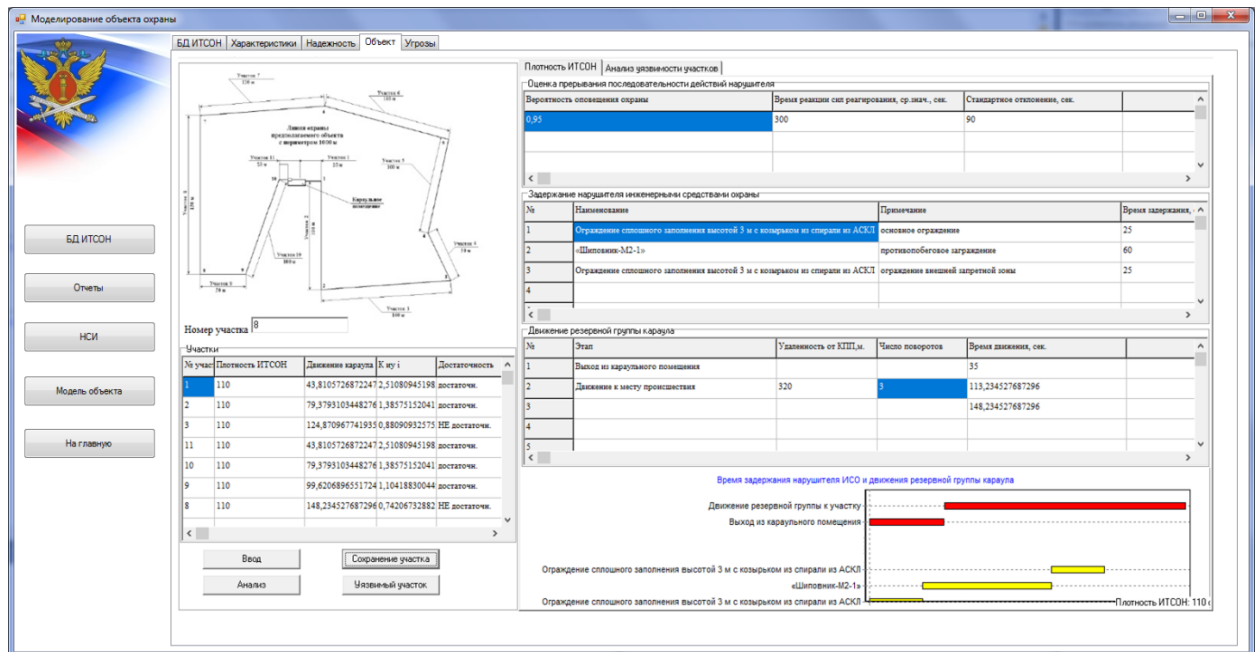


Рисунок 8 - Интерфейс построения оценки уязвимости периметра охраняемого объекта

В ходе выполнения процедуры оценки для каждого участка периметра на основе сравнения расчетных времен движения группы караула и движения нарушителя делается обоснованный вывод об уязвимости участков.

Применение такого программного средства в дальнейшем сможет обеспечить информационную, научно-обоснованную поддержку относительно принятия решений в области инженерной укреплённости объекта, технической оснащённости, обнаружительной способности и надёжности установленной на объекте УИС охранной системы. Таким образом, информационные технологии служат неотъемлемой частью процесса оценки эффективности охранных систем уголовно-исполнительной системы Российской Федерации. Дальнейшие работы в данном направлении представляют актуальную, практически значимую область исследований.

#### Список использованных источников

1. ГОСТ 34.003-99 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Доступ из справочно-правовой системы «КонсультантПлюс».
2. Гордин Г.Т., Алаухов С.Ф., Оленин Ю.А., О методах оценки эффективности систем физической защиты объектов. Проблемы объектовой охраны: Сб. научн. тр. – Вып. 2 – Пенза: Изд-во ИИЦ ПГУ.– 2001.

- 
3. Бояринцев А.В., Ничиков А.В., Редькин В.Б. Общий подход к разработке моделей нарушителей // Системы безопасности. – 2007. – № 4. – С. 50–53.
  4. Магуенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. – М.: Горячая линия – Телеком. – 2004. – 367 с.
  5. Сумин В.И., Чураков Д.Ю., Царькова Е.Г. Разработка моделей и алгоритмов информационных структур и процессов объектов особой важности// Сумин В.И., Чураков Д.Ю., Царькова Е.Г. Промышленные АСУ и контроллеры. 2019. № 4. С. 30-39.
  6. Чураков Д.Ю., Царькова Е.Г. Индивидуально-дифференцированный подход к подбору технических средств охраны и надзора для учреждений УИС// Чураков Д.Ю., Царькова Е.Г. В сборнике: Актуальные проблемы деятельности подразделений УИС Сборник материалов Всероссийской научно-практической конференции. Ответственный за выпуск Д.Г. Зыбин. 2018. С. 142-149.
  7. Чураков Д.Ю., Царькова Е.Г. Методы обработки экспертной информации при оптимизации управленческих решений в учреждениях уголовно-исполнительной системы// Чураков Д.Ю., Царькова Е.Г. В сборнике: Актуальные проблемы прикладной математики, информатики и механики сборник трудов Международной научно-технической конференции. Воронежский государственный университет. 2017. С. 1723-1734.
  8. Рычаго М.Е., Хорошева А.В. Математические методы оценки эффективности системы охраны исправительного учреждения // Вестник Владимирского юридического института. 2018. № 2 (47). С. 30-36.
  9. Измайлов А.В. Концептуальное проектирование интегрированных систем безопасности.// БДИ. Безопасность. Достоверность. Информация. – 1998. – №2. – С. 22-24.

*Для цитирования: Царькова Е.Г. Чем измерить эффективность: методы оценки эффективности систем физической защиты охраняемых объектов УИС // Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: сборник материалов круглого стола (24 июня 2019 года). С. 189-202.*