Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования

**Поволжский государственный университет
телекоммуникаций и информатики**

Кафедра экономических и информационных систем

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРОЕКТИРУЕМОЙ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТА

Методические указания
по выполнению контрольной работы по дисциплине
«Экономическая безопасность в корпоративных
информационных системах»

Составитель
д.т.н., профессор Маслов О.Н.

Самара, 2013

КОНТРОЛЬНАЯ РАБОТА

по дисциплине «Экономическая безопасность в корпоративных информационных системах»

ТЕМА: Оценка эффективности проектируемой системы защиты объекта.

ЗАДАНИЕ. Определить положение критической точки обнаружения (КТО) на предполагаемом маршруте движения злоумышленника по территории объекта и значение вероятности прерывания его действий $P_П$ при изменении условий работы системы защиты объекта (СЗО), соответствующих Вашему варианту изменения исходных данных относительного базового варианта.

БАЗОВЫЙ ВАРИАНТ. На рисунке 1 показан маршрут злоумышленника, целью которого хищения материалов (задокументированной информации) из контейнера, согласно которому на достижении цели злоумышленнику выделяется время 6 мин. при условии, что ему не помешают силы реагирования.

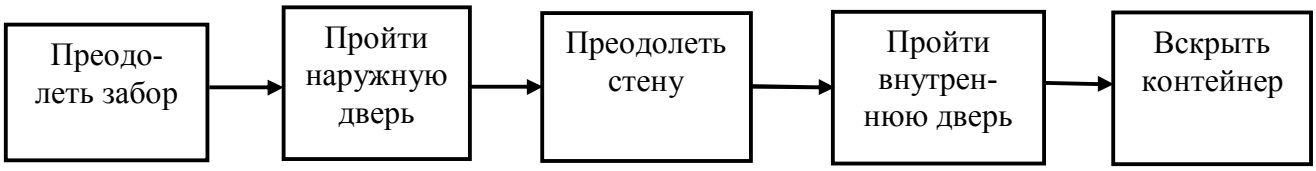

Рис. 1. Маршрут злоумышленника при движении к цели на территории объекта

В Таблице 1 представлены элементы задержки и обнаружения в составе СЗО на пути злоумышленника, которые он должен преодолеть или обойти.

Таблица 1. Исходные данные для базового варианта оценки эффективности проектируемой СЗО

Действия злоумышленника	**Элемент задержки**	**Элемент обнаружения**
Преодолеть забор	Материал забора	–
Пройти наружную дверь	Материал двери	Датчики на двери
Преодолеть стену	Материал стены	Охрана слышит шум
Пройти внутреннюю дверь	Материал двери	Датчики на двери
Вскрыть контейнер	Время, необходимое для вскрытия контейнера	Замок на контейнере

Таблица 2. Параметры элементов обнаружения и задержки элементов проектируемой СЗО

Действия злоумышленника	**Время $T_З$, сек**	$P_Н$ ($P_Д = 1 - P_Н$)	**Примечание**
Преодолеть забор	26	$P_Н^{(1)} = 1{,}0$	$P_П = 0{,}37$
Пройти наружную дверь	84	$P_Н^{(2)} = 0{,}9$	
Преодолеть стену	90	$P_Н^{(3)} = 0{,}7$	
Пройти внутреннюю дверь	110	$P_Н^{(4)} = 0{,}9$	$T_{З0} = 160$ сек.
Вскрыть контейнер	50	$P_Н^{(5)} = 0{,}8$	$T_Р = 140$ сек.

В Таблице 2 приведены параметры обнаружения (по вероятности P_H или $P_Д$) и задержки (по времени) для элементов СЗО, указанных в таблице 1.

Время реакции охраны T_P = 140 сек, указанное в таблице 2, на графике движения злоумышленника соответствует расположению КТ после стены перед внутренней дверью – так как в этой точке злоумышленнику для достижения цели необходимо время $T_{З0}$ = 160 сек (110 сек на преодоление двери и 50 сек на вскрытие контейнера), то есть $T_{З0} > T_P$ = 140 сек. Если СЗО не обнаружит злоумышленника у внутренней двери, перехватить его охрана уже не успеет.

На внешней ограде (забор) датчиков нет, поэтому вероятность необнаружения злоумышленника здесь равна 1; на наружной двери и стене датчики есть, на внутренней двери датчик есть, но от его срабатывания уже ничего не зависит, так как он расположен правее КТ (ближе к контейнеру).

Поэтому для базового варианта проектируемой СЗО вероятность прерывания $P_П$ = 1 – (1×0,9×0,7) = 0,37. Такое низкое значение $P_П$ (вероятности обнаружения злоумышленника в КТ, когда его перехват еще возможен) нельзя считать удовлетворительным. Поэтому Вам предлагается доработать проект СЗО и оценить его эффективность путем перерасчета $P_П$ и с учетом изменения положения КТ при следующих исходных данных.

1. Время реакции охраны в СЗО сокращено путем переноса поста ближе к контейнеру, теперь оно составляет

Вариант	1	2	3	4	5	6	7	8	9	10	11	12
T_P сек	120	115	110	105	100	95	90	85	80	75	70	65

2. Время, необходимое злоумышленнику для вскрытия контейнера, увеличено за счет установки сейфового замка и теперь оно равняется

Вариант	1	2	3	4	5	6	7	8	9	10	11	12
T_0 сек	130	125	120	115	110	105	100	95	90	85	80	75

3. Вероятность обнаружения $P_Д^{(2)} = 1 - P_H^{(2)}$ увеличена за счет установки на наружной двери более надежного и совершенного датчика, теперь она есть

Вариант	1	2	3	4	5	6	7	8	9	10	11	12
$P_Д^{(2)}$	0,35	0,40	0,45	0,50	0,55	0,60	0,65	0,70	0,75	0,80	0,85	0,90

4. Вероятность необнаружения $P_H^{(4)}$ необходимо будет учитывать, если условие $T_{З0} = T_0 > T_P$ выполняется в КТ, расположенной после внутренней двери, причем

Вариант	1	2	3	4	5	6	7	8	9	10	11	12
$P_H^{(4)}$	0,35	0,40	0,45	0,50	0,55	0,60	0,65	0,70	0,75	0,80	0,85	0,90

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ. Система защиты объекта (СЗО) представляет собой ***интегрированную совокупность компонентов*** (персонал, рабочие процедуры, оборудование), предназначенную для защиты корпоративной информационной системы от всех видов ***несанкционированных действий*** (НСД) потенциального злоумышленника, а также выполнять функцию его ***сдерживания*** (устрашения). Сдерживание достигается путем реализации мер, воспринимаемых злоумышленником как труднопреодолимые и делающие объект непривлекательным для него (охрана, освещение ночью, установка предостерегающих знаков, решетки на окнах, стальные двери и т.п.).

Основные «рабочие» ***компоненты СЗО*** – оборудование и охрана, главные ***функции СЗО*** – обнаружение, задержка и реагирование на действия злоумышленника в течение промежутка времени, меньшего чем то, которое необходимо ему для достижения цели. ***Критерии эффективности*** СФЗ являются измеряемыми и подлежат количественной оценке – расчетным и экспериментальным путем.

Обнаружение представляет собой установление факта появления злоумышленника на объекте, оно может быть скрытым и открытым. Показатели эффективности: значения вероятности правильного обнаружения $P_Д$ и вероятности прерывания $P_П$ действий злоумышленника. В функцию обнаружения СФЗ входит также ***контроль на входе***: разрешение санкционированного и выявление НСД людей и выноса имущества. Функцию обнаружения могут также выполнять охранники – размещенные на стационарных постах или патрулирующие территорию объекта.

Задержка – функция СЗО, которая состоит в том, что продвижение злоумышленника к цели замедляется с помощью барьеров, замков, привлечения персонала и т.п. Сотрудники охраны могут выполнять функцию задержки, если они расположены на хорошо защищенных местах. Показатель эффективности: время $T_З$, необходимое злоумышленнику для того, чтобы обойти каждый элемент задержки после его обнаружения (задержка злоумышленника до обнаружения представляет собой его сдерживание).

Реагирование состоит из действий, предпринимаемых охраной для прерывания действий злоумышленника. Прерывание определяется как прибытие достаточных сил охраны в нужное место для остановки (нейтрализации) злоумышленника, что предполагает получение ими точной информации о времени и месте нападения и возможность их развертывания. Развертывание включает в себя действия охраны между моментом получения ими информации о нападении и моментом их появления на позициях с целью прерывание действий злоумышленника.

Критическая точка (КТ) ***обнаружения*** (см. рис. 2) соответствует ситуации, когда остающееся время задержки $T_{З0}$ все еще превышает время реакции $T_Р$ – при этом ***вероятность прерывания*** $P_П$ есть суммарная вероятность обнаружения от начала пути до КТ, определяемой временем $T_{З0}$ (в отличие от суммарной вероятности обнаружения $P_Д$, соответствующей всему пути злоумышленника). Вероятность прерывания $P_П$ – ***общий критерий*** для оценки эффективности СФЗ, если силовые действия по нейтрализации злоумышленника не рассматриваются. Действия злоумышленника до КТ (осторожность, незаметность, скрытное проникновение, обман) и после КТ (уменьшение задержки, так как времени на реагирова-

ние у охраны все равно нет – злоумышленнику нужно только не медлить) показаны в верхней части рис. 2.

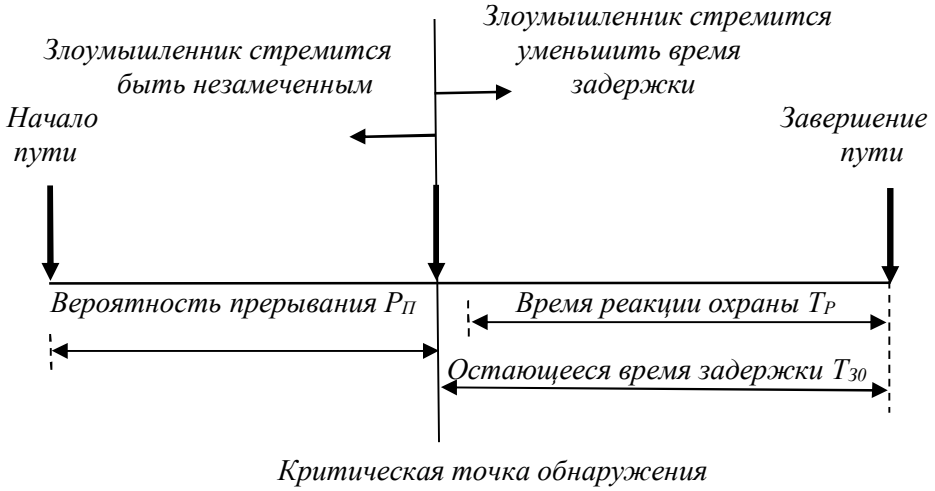

Рис. 2. К определению критической точки обнаружения (КТО) злоумышленника на территории объекта защиты

Считается, что после КТ злоумышленник ***может изменить тактику***: двигаться к цели с максимальной скоростью, обладая при этом всеми нужными знаниями, навыками и опытом преодоления преград, прибегая к применению силы, скрытности и обмана. На практике важно не дать злоумышленнику понять, что он перешел КТ – поэтому СЗО должна быть эшелонированной, адаптивной и гибкой.

В многоэлементной СЗО параметры времени задержки суммируются, а вероятности перемножаются: $T_З = \sum_{i=k}^{K} T_{Зi} > T_Р$; $P_П = 1 - \prod_{i=k}^{K} P_{Нi}$, где K – общее число элементов СЗО на пути злоумышленника; k – «номер» точки на маршруте, где $T_З$ начинает превышать $T_Р$, k [1; K]; $T_{Зi}$ – время задержки i-го элемента СЗО; $P_{Нi}$ – вероятность того, что i-ый элемент СЗО не обнаружит злоумышленника. Значения времени задержки для рассматриваемых элементов СЗО указаны в таблице 2, вероятность прерывания в данном случае равна $P_П = 1 - P_Н^{(1)} \times P_Н^{(2)} \times P_Н^{(3)} \times P_Н^{(4)}$.

Дополнительная литература

1. Гарсиа М. Проектирование и оценка систем физической защиты. Пер с англ. М.: Мир-АСТ, 2003. – 386 с.

2. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. М.: Горячая линия – Телеком, 2004. – 367 с.

3. Барсуков В.С. Обеспечение информационной безопасности. М.: ТЭК, 1996.

5. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999.