

DOI: 10.24143/2072-9502-2017-3-31-39
УДК 654.9:004.7.056

Ш. Г. Магомедов, В. Ф. Шуршев, Г. А. Попов, А. Ф. Дорохов, М. Ф. Руденко

ПОСТРОЕНИЕ МОДЕЛЕЙ ОПИСАНИЯ РИСКОВ ОХРАННЫХ ДЕЙСТВИЙ ПО ЗАЩИТЕ ВНЕШНИХ ПЕРИМЕТРОВ ОРГАНИЗАЦИИ

Рассматривается задача оценки издержек и потерь, связанных со степенью защищенности внешних параметров объекта защиты от возможных несанкционированных действий, на основе построения математической модели. Выделены две основные составляющие, связанные с охраной объектов: служба охраны, опирающаяся на действия охранных групп, и служба технической охраны, опирающаяся на использование современных технических средств охраны. Получены соотношения для средних издержек и потерь, связанных с каждой из этих служб, а также для вероятностей того, что нарушитель сможет преодолеть внешний периметр объекта, несмотря на попытки противодействия указанных служб. Введены новые характеристики системы защиты – показатели надежности и квалификации сотрудника службы охраны, которые учитываются в процессе оценок. Продемонстрирована возможность использования эвристических выводов при анализе слабоструктурированных характеристик, каковыми являются многие вероятности, связанные с охранными действиями. Полученные соотношения могут быть использованы для постановки и решения задачи минимизации потерь, связанных с обеспечением охранной деятельности на объекте защиты по претотвращению злоумышленных действий.

Ключевые слова: объект защиты, охрана периметров, охранный персонал, технические средства охраны, суммарные издержки и потери, вероятность нарушения, построение модели.

Введение

Обеспечение сохранности и защищенности людей и имущества в заданной зоне контроля (в частности, территории организации и личного домовладения), несмотря на огромный исторический опыт решения этой проблемы, по-прежнему остается актуальной. Даже использование современных сложных систем и технологий (например, типа «умный дом»), систем спутниковой навигации (GPS и ГЛОНАСС) не позволяет обеспечить окончательное решение данной проблемы. Потенциальные злоумышленники часто рано или поздно находят пути преодоления всех хитроумных преград, осложняющих доступ к ценностям (в частности, информационным), находящимся на охраняемой территории. В связи с этим необходимо констатировать и принять как базовую аксиому положение, что практически невозможно полностью закрыть ни один из каналов возможного проникновения на объект защиты. Как следствие, более реальной является следующая позиция – следует стремиться не к абсолютному закрытию возможных каналов злоумышленного проникновения, а к минимизации средних суммарных издержек, связанных с возможным злоумышленным проникновением на объект защиты. В настоящее время во многих сферах деятельности (экономика, информационная безопасность и др.) в качестве меры средних издержек для каждого канала злоумышленного проникновения рассматриваются риски, связанные со средними возможными потерями по этим каналам. Именно поэтому проблема оценки рисков для различных возможных каналов злоумышленного проникновения является актуальной.

Важной неотъемлемой частью большинства объектов защиты является наличие специальной системы охраны. Ниже рассматривается случай стационарного объекта защиты (контролируемой территории помещения), поэтому система охраны обычно включает наличие специальных охранных групп, которые также являются возможными каналами злоумышленных действий по отношению к объекту защиты. Рассматриваются методы оценки рисков, связанных с указанными охранными системами.

Цель исследования – решение задачи по оценке издержек и потерь, связанных с уровнем защищенности внешних параметров объекта защиты от возможных несанкционированных действий, на основе построения математической модели, позволяющей описать потери и затраты в процессе осуществления охранных действий по защите внешних периметров объекта.

Среди исследований по указанной тематике выделим работы [1–5]. Однако предлагаемая постановка математической формализации указанной задачи ранее в доступной литературе не встречалась.

Оценки для рисков, связанных с охранными группами

Отметим, что технологии охраны внешнего периметра объекта защиты и его внутренней территории, несмотря на их общее сходство, имеют некоторые существенные различия как по характеру угроз и выполняемых действий, так и по составу технических средств охраны. В связи с этим указанные два аспекта охранных действий требуют отдельного рассмотрения. Рассматриваться будет периметровая охрана объекта. Выделим два основных класса охранных мероприятий и действий: *организационные меры защиты* (регламент использования охранных групп, нахождение на объекте защиты и перемещения по нему и др.) и *технические средства защиты* (системы видеонаблюдения и охранной сигнализации, включающие датчики и устройства сигнализации разных типов (инфракрасные, перемещения, датчики разбития стекол, раскрытия дверей и др.)). Исходя из этого, выделим два направления исследования – *охранная группа и инженерно-технические средства охраны* – и связанные с ними компоненты охранной системы. Опишем основные факторы, порождающие потери, издержки и связанные с этим риски для каждой из выделенных групп компонентов.

Основными факторами, которые могут породить потери, связанные с *охранной группой*, являются: 1) уровень профессиональной квалификации части персонала охранной группы ниже приемлемого; 2) малое количество сотрудников с учетом длины периметра и сложности его охраны; 3) недобросовестное выполнение должностных обязанностей отдельными сотрудниками и даже преступный сговор с ними.

Введем обозначения:

– p_G – вероятность того, что нарушителю удастся преодолеть систему внешней охраны объекта;

– $L^{(G)}$ – средние потери, которые ожидаются в случае преодоления нарушителем системы охраны внешнего периметра объекта защиты.

Вероятность p_G определяется следующими характеристиками системы охраны и описывается некоторой функцией, зависящей от этих характеристик:

– $c_k^{(Q)}$ ($k = \overline{1; N_G}$) – уровень профессиональной квалификации k -го сотрудника группы охраны внешнего периметра объекта, где N_G – число членов охранной группы;

– l_{Pr} – средняя длина участка внешнего периметра, приходящаяся на одного сотрудника группы охраны;

– r_k – надежность k -го сотрудника группы охраны при выполнении должностных обязанностей;

– $\lambda_j^{(inf)}$ – ожидаемое среднее количество нарушений j -го вида в течение одного года, для определения которого используется следующая шкала уровней нарушений: незначительные нарушения ($j = 0$), в частности попытки проникновения на территорию объекта с целью хищения в незначительных размерах; крупные хищения, осуществляемые без контактов со службой охраны ($j = 1$); крупные хищения, при которых происходит столкновение с группой охраны или нейтрализация технических средств охраны ($j = 2$); объекта;

– w – погодные условия в зоне охраны.

Суммарные средние потери (риски) L_G , связанные с охранной группой, могут быть оценены на основе соотношения

$$R_G = p_G \cdot L^{(G)},$$

где, как было указано выше,

$$p_G = \varphi(l_{Pr}, c_k^{(Q)}, r_k (k = \overline{1; N_G}), \lambda_j^{(inf)} (j = 0, 1, 2), w) \quad (1)$$

и $\varphi(\cdot)$ – некоторая функция от перечисленных выше переменных, приемлемое выражение для вычисления значений которой необходимо найти.

Применительно к *инженерно-техническим средствам охраны* введем следующие характеристики:

- d_k ($k = \overline{1; N_d}$) – весовой коэффициент, характеризующий степень опасности несанкционированного нарушения режима охраны внешнего периметра объекта на k -м участке;
- N_d – количество выделенных участков периметра объекта в системе технической охраны внешнего периметра объекта;
- u_{vis} – площадь территории, примыкающей к периметру охраняемого объекта защиты, которая просматривается с приемлемым качеством с помощью средств видеонаблюдения;
- s_k ($k = \overline{1; N_d}$) – наличие системы охранной сигнализации на k -м участке внешнего периметра;
- $p_{вдн}$ – вероятность обнаружения с помощью средств видеонаблюдения.

Тогда средние издержки, которые ожидаются в случае успешного преодоления злоумышленником систем инженерно-технической охраны внешнего периметра, оцениваются следующим образом:

$$R_T = p_T \cdot L^{(T)},$$

где $L^{(T)}$ – средние потери, которые ожидаются в случае, если нарушитель смог преодолеть инженерно-технические средства охраны. При этом

$$p_T = \theta(l_{пр}, p_{вдн}, d_k^j, s_k(k = \overline{1; N_d}), \lambda_j^{(нар)}(j = 0, 1, 2)), \quad (2)$$

и $\theta(\cdot)$ – некоторая функция, для которой необходимо найти приемлемое выражение.

Таким образом, для оценки суммарных потерь, связанных с системой охраны внешних периметров, необходимо прежде всего описать возможный вид функций $\varphi(\cdot)$ и $\theta(\cdot)$ – назовем эти функции вычислительными.

Анализ выражений для вычислительных функций

Ниже, при выводе выражений (3) и (4) для функций $\varphi(\cdot)$ и $\theta(\cdot)$ (см. (1) и (2)), вводятся некоторые дополнительные предположения. Прежде всего введем следующую шкалу измерения уровня квалификации сотрудника охранной группы. Предлагается четырехуровневая система оценки.

Первый уровень ($c_k^{(Q)} = 1$): сотрудник охранной службы не способен в ответственных ситуациях нейтрализовать злоумышленника или остановить его, например, в силу низкого уровня физической готовности, либо склонности к взяткам и коррупционным комбинациям, либо отсутствия желания выполнять должностные обязанности на требуемом уровне, либо способен нарушать требования, установленные в регламентных документах по охране (в частности, может отсутствовать на рабочем месте, быть невнимательным, заниматься вымогательством).

Второй уровень ($c_k^{(Q)} = 2$): сотрудник охранной службы выполняет должным образом свои должностные обязанности только тогда, когда либо находится под контролем, либо информация об эффективности его работы может стать достоянием руководства; в случае отсутствия перечисленных обстоятельств ненадежен, склонен к коррупционным схемам.

Третий уровень ($c_k^{(Q)} = 3$): сотрудник охранной службы в целом компетентен, надежен и добросовестно относится к своим рабочим обязанностям, но в силу личных качеств может нарушить их (например, в отношении знакомых ему людей), поэтому нет должной гарантии и уверенности, что в ответственных ситуациях он все выполнит на должном уровне.

Четвертый уровень ($c_k^{(Q)} = 4$): сотрудник охранной службы – профессионал высокой квалификации, т. е. хорошо знает и добросовестно выполняет свои должностные обязанности, имеет большой стаж работы, находится в хорошей физической и психологической форме, способен

проявить разумную инициативу, адекватно и рационально действовать при возникновении нестандартной или опасной ситуации.

Для нахождения искомых функций получим соотношения для ряда вероятностей.

Рассмотрим вероятность $p_{зп}$ того, что злоумышленники смогут преодолеть систему охраны объекта хотя бы на одном из участков внешнего периметра. Введем обозначения:

- $S_{оп}$ – объем средств, выделяемых на охрану периметра;
- $z_{кн}$ и $z_{кн} \alpha_{оз}$ – длина периметровой зоны контроля одним охранником для неопасной и опасной зон, где $\alpha_{оз} < 1$ – корректирующий коэффициент, определяющий степень уменьшения зоны контроля для опасных участков периметра;
- $e_{ок}$ – средние полные затраты на одного охранника, включая его оснащение;
- $p_{ок}$ – вероятность того, что охранник не воспрепятствует нарушению, связанному с пересечением охраняемого периметра;
- N_3 и $N_{оз}$ – число всех и опасных зон соответственно.

Тогда справедливо равенство $(N_3 - N_{оз}) z_{кн} + N_{оз} z_{кн} \alpha_{оз} = l_{пр}$, откуда следует:

$$N_3 = (l_{пр} + N_{оз} z_{кн}) / z_{кн}.$$

Исходя из затрат, находим, что среднее число охранников, которое выделяется на контроль периметра, равно $N_{оп} = S_{оп}/e_{ок}$. Считая, что у злоумышленника нет данных о параметрах контролируемости конкретного участка периметра, заключаем, что вероятность преодоления злоумышленником периметра объекта, равна:

$$p_{зп} = (N_{оп} / N_3) p_{ок} = (S_{оп} z_{кн}) / ((l_{пр} + N_{оз} z_{кн}) e_{ок}) p_{ок}. \quad (3)$$

Следующая вероятность, которая потребуется ниже, – это вероятность убийства $p_{уп}$ злоумышленников из зоны контроля внешнего периметра до момента прибытия сотрудников охраны в зону контроля. В этом случае сотрудник службы охраны может самостоятельно, не нарушая законодательных и нормативных требований и ограничений, предпринять меры по задержанию хотя бы одного из злоумышленников – обозначим вероятность успешного действия охранника как $p_{зо}$. Благодаря задержанию злоумышленника, в дальнейшем возможна нейтрализация последствий злоумышленной атаки (например, возмещение ущерба, возвращение похищенных ценностей и т. п.) с вероятностью $p_{взв}$. Тогда вероятность того, что злоумышленникам удастся без последствий для них завершить свою атаку, равна

$$P_{уп} = 1 - p_{зо} \cdot p_{взв}. \quad (4)$$

На основе анализа возможных вариантов по противодействию злоумышленным атакам получаем следующее выражение для вероятности P_{yx} того, что злоумышленная атака окажется для злоумышленников успешной:

$$P_{yx} = P_{зп} P_{уп} = \frac{S_{оп} z_{кн}}{(l_{пр} + N_{оз} \alpha_{оз} z_{кн})} p_{ок} (1 - p_{зо} p_{взв}). \quad (5)$$

Из формул (3)–(5) заключаем, что рассматриваемые вероятности зависят от квалификации и надежности каждого из сотрудников охранной группы охраны, а также от их способности задержать нарушителя до прибытия представителей силовых ведомств.

Вероятность $p_{ок}$ зависит, в частности, от квалификации и добросовестности (надежности) выполнения сотрудником службы охраны своих обязанностей. Обозначим уровни квалификации и надежности сотрудника как x и y соответственно. Эти характеристики могут быть измерены по шкале натуральных чисел от 1 до $N_{квал}$ и $N_{над}$ соответственно, где $N_{квал}$ и $N_{над}$ – максимально возможные значения соответствующих уровней. Примем: чем меньше x или y , тем ниже квалификация или добросовестность соответственно. Далее, обозначим как $p_{нач}$ значение вероятности $p_{ок}$ для наиболее крайнего случая, когда нарушение не нейтрализовано начинающим сотрудником, т. е. не имеющим опыта охранной работы. Естественно принять в этом случае значения уровней квалификации x и надежности y равными 1. Вероятность $p_{нач}$ можно представить в виде суммы двух слагаемых: первое слагаемое $p_{нач.хл}$ учитывает случаи, когда злонамеренное действие осу-

ществляется спонтанно, т. е. не подготовлено заранее (например, хулиганский поступок), а второе слагаемое $p_{\text{нач.зн}}$ – когда злонамеренное действие является результатом реализации заранее подготовленного плана. Тогда перечисленные вероятности связаны равенством

$$p_{\text{нач}} = \frac{\mu_{\text{хл}}}{\mu_{\text{хл}} + \mu_{\text{зн}}} p_{\text{нач.хл}} + \frac{\mu_{\text{зн}}}{\mu_{\text{хл}} + \mu_{\text{зн}}} p_{\text{нач.зн}},$$

где в качестве оценок для $\mu_{\text{хл}}$ и $\mu_{\text{зн}}$ можно взять среднее количество хулиганских и злонамеренных правонарушений в зоне, примыкающей к организации, либо в районе нахождения организации в течение определенного (обычно регламентного) промежутка времени.

Получим на основе эвристических рассуждений выражения для оценки вероятности $p_l^{NS} = p_l^{NS}(x_l, y_l)$ того, что l -й сотрудник службы охраны, у которого уровень квалификации равен x_l , а уровень надежности y_l , не сможет нейтрализовать нарушителя. Примем следующее допущение: при увеличении квалификации x или надежности y сотрудника на одну единицу эффективность его работы увеличивается в $d_{\text{квал}}$ и $d_{\text{над}}$ раз соответственно, причем коэффициенты $d_{\text{квал}}$ и $d_{\text{над}}$ не зависят от x и y . Здесь эффективность измеряется коэффициентом, описывающим уменьшение вероятности того, что злоумышленник сможет преодолеть зону охраны, контролируруемую данным сотрудником службы охраны. Тогда при уровнях квалификации x и надежности y указанный коэффициент эффективности работы сотрудника (т. е. уменьшение указанной вероятности) по отношению к начинающему сотруднику будет равен

$$\left(1 + \frac{t_{\text{квал}}}{100}\right)^{-(x_l-1)} \left(1 + \frac{t_{\text{над}}}{100}\right)^{-(y_l-1)},$$

где $1 + \frac{t_{\text{квал}}}{100} = d_{\text{квал}}$, $1 + \frac{t_{\text{над}}}{100} = d_{\text{над}}$ и $t_{\text{квал}}$ и $t_{\text{над}}$ – есть величина (%), на которую увеличивается эффективность работы сотрудника в случае увеличения уровня квалификации или надежности на одну единицу. Отсюда, на основе принятых определений, выводится следующее равенство для вероятности того, что l -й охранник, имеющий уровень квалификации x_l и уровень надежности y_l , не остановит злоумышленника:

$$p_l^{NS}(x_l, y_l) = (1 - p_{\text{нач}}) \left(1 + \frac{t_{\text{квал}}}{100}\right)^{-(x_l-1)} \left(1 + \frac{t_{\text{над}}}{100}\right)^{-(y_l-1)}. \quad (6)$$

Приведенное соотношение обеспечивает выполнение следующей зависимости: чем выше уровень квалификации и степень надежности сотрудника, тем меньше вероятность того, что он не сможет задержать нарушителя.

Пусть $\tau_{\text{пол}}$ – есть средняя длительность промежутка времени, через который в зону нарушения прибудет охранная группа или наряд полиции. Длительность времени, в течение которого сотрудник службы охраны окажется способным удерживать нарушителя (или нарушителей) в зоне охраны, убывает; примем, что скорость этого убывания подчиняется экспоненциальному закону, т. е. экспоненциально уменьшается вероятность того, что сотрудник сможет контролировать нарушителя. Тогда, при уровне надежности сотрудника y , можно считать: вероятность того, что сотрудник службы охраны окажется способным контролировать хотя бы одного нарушителя в течение промежутка времени t , будет описываться выражением $\exp\{-\delta_{\text{сдер}} y t\}$, где $\delta_{\text{сдер}}$ – коэффициент, учитывающий индивидуальные особенности ситуации (места, времени года и суток и др.), когда происходит нейтрализация нарушителя. Отсюда, используя соотношение (6), записываем следующее соотношение для вероятности $\pi(l)$ того, что l -й охранник, имеющий уровень квалификации x_l и уровень надежности y_l , не задержит нарушителя до момента появления охранной группы или полиции:

$$\pi(l) = (1 - p_{\text{нач}}) \left(1 + \frac{t_{\text{квал}}}{100}\right)^{-(x_l-1)} \left(1 + \frac{t_{\text{над}}}{100}\right)^{-(y_l-1)} (1 - \exp\{-\delta_{\text{сдер}} y_l \tau\}). \quad (7)$$

Примем, что нахождение каждого сотрудника службы охраны в зоне нарушения является полностью случайным, т. е. вероятность того, что данный охранник окажется в зоне нарушения, равна $1/N_{\text{оп}}$. Отсюда, с учетом (5) и (7), получаем следующее выражение для оценки значений функции $\varphi(\cdot)$:

$$\varphi(x_l, y_l, l = \overline{1; N_{\text{оп}}}; S_{\text{оп}}; \tau; \mu_{\text{хл}}; \mu_{\text{зн}}) = \frac{1}{N_{\text{оп}}} \sum_{l=1}^{N_{\text{оп}}} \pi(l) = \frac{1}{N_{\text{оп}}} \sum_{l=1}^{N_{\text{оп}}} (1 - p_{\text{нач}}) \times \\ \times \left(1 + \frac{t_{\text{квал}}}{100}\right)^{-(x_l-1)} \left(1 + \frac{t_{\text{над}}}{100}\right)^{-(y_l-1)} (1 - \exp\{-\delta_{\text{сдер}} y_l \tau\}).$$

Управляемыми параметрами функции $\varphi(\cdot)$, т. е. параметрами, значения которых можно целенаправленно изменять, являются $p_{\text{нач}}$, $e_{\text{опр}}$, $z_{\text{кн}}$, $t_{\text{квал}}$, $t_{\text{над}}$, $\delta_{\text{сдер}}$, что важно при построении системы контроля и управления процессом охраны внешних периметров.

Выражение для функции $\theta(\cdot)$ находится аналогичным образом. Напомним: функция $\theta(\cdot)$ описывает вероятность того, что нарушители не смогут преодолеть зону технической охраны. Чтобы получить выражение для $\theta(\cdot)$, введем следующие обозначения:

– $N_{\text{тп}}$ – число технических средств (например, видеокамер), функционирующих в зоне контроля внешнего периметра объекта защиты;

– $N_{\text{тз}}$ – среднее число технических средств охраны в одной обычной (неопасной) зоне периметра;

– $l_{\text{пз}}$ – длина участка периметра, который может надежно и устойчиво контролироваться с помощью одного технического средства (в частности, с помощью одной видеокамеры);

– v – количество опасных зон;

– $\alpha_{\text{тз}} > 1$ – коэффициент, характеризующий степень увеличения плотности технических средств охраны в опасной или особой зоне.

Тогда, совершенно так же, как и при выводе соотношения (3), получаем выражение для вероятностей $p_{\text{тп}}$ того, что нарушитель не сможет преодолеть систему технической охраны периметра объекта защиты. Для этого прежде всего найдем выражение, описывающее взаимосвязь между числом неопасных и опасных зон периметра. Справедливо соотношение

$$N_{\text{тп}} = N_{\text{тз}} \left(\frac{l_{\text{пз}}}{l_{\text{пз}}} - v \right) + \alpha_{\text{тз}} N_{\text{тз}} v,$$

откуда получаем

$$N_{\text{тз}} = N_{\text{тп}} / \left(\frac{l_{\text{пз}}}{l_{\text{пз}}} - (1 - \alpha_{\text{тз}}) v \right). \quad (8)$$

Известно, что степень просматриваемости объектов (линейно зависящая от мощности падающего на них светового потока) обратно пропорциональна квадрату расстояния до этих объектов, т. е. справедливо следующее соотношение для вероятности $p_{\text{пз}}$ выявления объекта:

$$p_{\text{пз}} = \frac{\gamma_{\text{тех}} \lambda w}{(l_{\text{пз}})^2}, \quad \text{где } \lambda \text{ – степень освещенности зоны периметра } (0 \leq \lambda \leq 1), \quad w (0 \leq w \leq 1) \text{ – степень}$$

прозрачности воздуха в зоне просмотра с учетом погодных-климатических и техногенных условий (ухудшающихся при наличии дождя, дыма, снега, пыли и др.); $\gamma_{\text{тех}}$ – коэффициент, учиты-

вающий технические параметры видеокамеры. Для простоты примем, что все видеокамеры на объекте защиты одного типа. Тогда вероятность того, что подозрительный объект будет обнаружен в зоне периметра хотя бы одной видеокамерой (или техническим устройством) в обычной и опасной зонах периметра равна соответственно:

$$p_{\text{обн.норм}} = 1 - (1 - p_{\text{пз}})^{N_{\text{тз}}} = 1 - \left(1 - \frac{\gamma_{\text{тех}} \lambda w}{1 + (l_{\text{пз}})^2} \right)^{N_{\text{тз}}}, \quad (9)$$

$$p_{\text{обн.оп}} = 1 - (1 - p_{\text{пз}})^{\alpha_{\text{тз}} N_{\text{тз}}} = 1 - \left(1 - \frac{\gamma_{\text{тех}} \lambda w}{1 + (l_{\text{пз}})^2} \right)^{\alpha_{\text{тз}} N_{\text{тз}}}. \quad (10)$$

На основе соотношений (9) и (10) получаем следующее выражение для вероятности того, что нарушитель не сможет преодолеть данный участок зоны технической охраны:

$$p_{\text{тп}} = 1 - (1 - p_{\text{обн.норм}})^{\frac{l_{\text{нпр}}}{l_{\text{гп}} - v}} (1 - p_{\text{обн.оп}})^v. \quad (11)$$

Соотношения (8)–(11) позволяют записать формулу для оценки вероятности обнаружения нарушителя с помощью технических средств охраны при его попытке пересечь внешний периметр объекта:

$$p_{\text{тех.пер.}} = 1 - (1 - p_{\text{обн.норм}})^{\frac{l_{\text{нпр}}}{l_{\text{просм.зон}} - v}} (1 - p_{\text{обн.оп}})^v. \quad (12)$$

Соотношение (11) с учетом (12) позволяет записать следующее выражение для функции $\theta(\cdot)$:

$$\begin{aligned} \theta(x_i, y_i, l = \overline{1}; N_{\text{оп}}^{(i)}; s_{\text{зон}}^{(i)}, i \in D; S_{JG}; l_{\text{пр}}; \lambda; w) = \\ = 1 - (1 - p_{\text{обн.норм}})^{\frac{l_{\text{пр}}}{l_{\text{нгп}} - v}} (1 - p_{\text{обн.оп}})^v \prod_{j \in D} (1 - p_{\text{обн.оп}}^{(j)}) = \\ = 1 - \left(1 - \frac{\gamma_{\text{тех}} \lambda w}{1 + (l_{\text{пз}})^2} \right)^{N_{\text{тз}} \left(\frac{l_{\text{пр}}}{l_{\text{нгп}} - v} \right)} \left(1 - \frac{\gamma_{\text{тех}} \lambda w}{1 + (l_{\text{гп}})^2} \right)^{\alpha_{\text{тз}} N_{\text{тз}} v} \prod_{i \in D} \left(1 - \frac{\gamma_{\text{тех}} \lambda_i w_i}{1 + s_{\text{зон}}^{(i)}} \right)^{N_{\text{тех.зон}}^{(i)}}. \end{aligned}$$

Управляемыми параметрами функции $\theta(\cdot)$ являются: $\gamma_{\text{тех}}$, $N_{\text{тз}}$, $l_{\text{пз}}$, $\alpha_{\text{тз}}$, $N_{\text{тз}}^{(i)}$ ($i \in D$).

Оценка перечисленных параметров в значительной степени индивидуальна для каждого объекта защиты и поэтому должна производиться непосредственно на объекте защиты с использованием различных методов экспериментального, сравнительного и экспертного характера. В дальнейшем предполагается разработать методику проведения оценки перечисленных параметров.

Отметим также, что наличие управляемых параметров, входящих в состав функций $\varphi(\cdot)$ и $\theta(\cdot)$, позволяет поставить задачу нахождения оптимального варианта организации системы охраны объекта и управления им.

Заключение

В ходе исследования:

- проведена оценка суммарных потерь, связанных с обеспечением охраны некоторого объекта с целью его защиты от злоумышленных и иных деструктивных действий;
- получены соотношения для функций потерь, связанных с преодолением злоумышленником внешнего периметра охраны и проникновением к материальным ценностям на объекте защиты;
- проведен анализ возможного вида двух вспомогательных функций, введенных при построении функций потерь.

Полученные соотношения могут быть использованы для постановки и решения задачи минимизации потерь, связанных с обеспечением охранной деятельности на объекте защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Белов С. В., Мельников А. В. Процедура оценки показателей злоумышленного проникновения в составе автоматизированной системы контроля физической безопасности объекта защиты // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2014. № 2. С. 28–37.
2. Попов Г. А., Белов С. В. Оценка степени физической защищенности объект защиты // Изв. вузов. Сев.-Кавказ. регион. Техн. науки. 2005. № 2. С. 3–6.
3. Магауенов Р. Г., Семёнов О. И., Афанасьева Л. Г., Егоров А. Н. Толковый словарь терминов по системам физической защиты. М.: Security Focus, 2008. 288 с.
4. Рыкунов В. Охранные системы и технические средства физической защиты объектов. М.: Security Focus, 2011. 288 с.
5. Гарсия М. Проектирование и оценка систем физической защиты. М.: Мир, 2003. 392 с.

Статья поступила в редакцию 02.06.2017

ИНФОРМАЦИЯ ОБ АВТОРАХ

Магомедов Шамиль Гасангусейнович – Россия, 119454, Москва; Московский технологический университет; канд. техн. наук; зав. кафедрой автоматизированных систем управления; msgg@list.ru.

Шуршев Валерий Фёдорович – Россия, 414056, Астрахань; Астраханский государственный технический университет; г-р техн. наук, профессор; профессор кафедры прикладной информатики; v.shurshhev@mail.ru.

Попов Георгий Александрович – Россия, 414056, Астрахань; Астраханский государственный технический университет; г-р техн. наук, профессор; зав. кафедрой информационной безопасности; popov@astu.org.

Дорохов Александр Фёдорович – Россия, 414056, Астрахань; Астраханский государственный технический университет; г-р техн. наук, профессор; профессор кафедры судостроения и энергетических комплексов морской техники; dorokhovaf@gambler.ru.

Руденко Михаил Фёдорович – Россия, 414056, Астрахань; Астраханский государственный технический университет; г-р техн. наук, профессор; профессор кафедры безопасности жизнедеятельности и инженерной экологии; mf.rudenko@mail.ru.



S. G. Magomedov, V. F. Shurshhev, G. A. Popov, A. F. Dorokhov, M. F. Rudenko

BUILDING RISK MODELS FOR DESCRIBING SECURITY FUNCTIONS ON PROTECTING OUTER PERIMETERS OF THE ORGANIZATION

Abstract. The paper considers the problem of estimating the costs and losses associated with the degree of protection of the external perimeters of the object of protection against possible unauthorized actions, based on the construction of a mathematical model. Two main components related to the protection of objects have been identified: security service based on the activities of security groups; technical protection service based on the use of modern technical means of protection. The authors have obtained the relations for the average costs and losses associated with each of these services, as well as for the likelihood that the violator will be able to overcome the external prime-

ter of the object, despite attempts to counteract these services. New characteristics of the protection system have been introduced - indicators of reliability and qualifications of the security officer, which are taken into account in the assessment process. The possibility of using heuristic conclusions in the analysis of weakly structured characteristics, such as many of the probabilities associated with security actions, has been demonstrated. The obtained relationships can be used for setting and solving the problem of minimizing losses associated with providing security activity at the protection object to prevent malicious acts.

Key words: object of protection, perimeters protection, security group, technical means of protection, total costs and losses, probability of violation, model building.

REFERENCES

1. Belov S. V., Mel'nikov A. V. Protседura otsenki pokazatelei zloumyshlennogo proniknoveniia v sostave avtomatizirovannoi sistemy kontroliа fizicheskoi bezopasnosti ob"ekta zashchity [The procedure of evaluation of indicators of malicious penetration in the structure of the automated monitoring system of physical security of the protected object]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naia tekhnika i informatika*, 2014, no. 2, pp. 28-37.
2. Popov G. A., Belov S. V. Otsenka stepeni fizicheskoi zashchishchennosti ob"ekt zashchity [Assessment of physical protection level of the protection object]. *Izvestiia vuzov. Severo-Kavkazskii region. Tekhnicheskie nauki*, 2005, no. 2, pp. 3-6.
3. Magauenov R. G., Semenov O. I., Afanas'eva L. G., Egorov A. N. *Tolkovyi slovar' terminov po sistemam fizicheskoi zashchity* [Explanatory dictionary of the physical protection systems terminology]. Moscow, Security Focus Publ., 2008. 288 p.
4. Rykunov V. *Okhrannye sistemy i tekhnicheskie sredstva fizicheskoi zashchity ob"ektov* [Protection systems and technical means of physical protection of the object]. Moscow, Security Focus Publ., 2011. 288 p.
5. Garcia M. L. *Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann, 2001. 370 p. (Russ. ed.: Garsia M. Proektirovanie i otsenka sistem fizicheskoi zashchity. Moscow, Mir Publ., 2003. 392 p.).

The article submitted to the editors 02.06.2017

INFORMATION ABOUT THE AUTHORS

Magomedov Shamil Gasanguseinovich – Russia, 119454, Moscow; Moscow Technological University; Candidate of Technical Sciences; Head of the Department of Automated Control Systems; msgg@list.ru.

Shurshev Valeriy Fedorovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Professor of the Department of Applied Informatics; v.shurshev@mail.ru.

Popov Georgiy Aleksandrovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Head of the Department of Information Security; popov@astu.org.

Dorokhov Alexander Fedorovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Professor of the Department of Shipbuilding and Power Complexes of Marine Engineering Equipment; dorokhovaf@rambler.ru.

Rudenko Mikhail Fedorovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Professor of the Department of Life Security and Engineering Ecology; mf.rudenko@mail.ru.

