Список использованной литературы: ***1.*** *Рамишвили Г. С. Автоматическое опознавание говорящего по голосу. // М.: Радио и связь, 1981. – 224 с.* ***2.*** *Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. // М: Мир, 1978. – 848 с.* ***3.*** *Темников В. А., Шарий Т. В., Темникова Е. Л., Конфорович И. В. Голосовая аутентификация операторов, использующих в процессе работы нормативно установленную фразеологию // Інформаційна безпека. – 2011. – №1(5). – С.125-130.* ***4.*** *Темников В. А., Темникова Е. Л., Конфорович И. В. Выбор параметров системы аутентификации человека по голосу // Інформаційна безпека. – 2012.– №2(8). – С.151-157.* ***5.*** *Donoho, D. L. De-Noising by soft-thresholding // IEEE Trans. on Inform. Theory. - Vol.41. - №3. - 1995. - P.613-627.* ***6.*** *Смоленцев Н. К. Основы теории вейвлетов. – М.: ДМК, 2005. − 303 с.* ***7.*** *Темников В. А., Пономаренко Л. В. Методика проведения шумоочистки речевого сигнала в процессе распознавания // Вестник Восточноукраинского национального университета им. В. Даля. - №5 (111). – Ч.1. – 2007. – С.123-127.* ***8.*** *Астафьева Н. М. Вейвлет-анализ: основы теории и примеры применения // Успехи физических наук. – 1996. – Т.166. – №11. – С. 1145-1170.* ***9.*** *Баевский Р. М. Анализ вариабельности сердечного ритма: история и философия, теория и практика // Клиническая информатика и телемедицина. - 2004. – №1.- С. 54-64.* ***10.*** *Кальниш В. В., Романенко Е. В., Самойлов В. Д. Архитектура системы и разработка программных средств автоматизации диагностики психологических и психофизиологических качеств оперативно-диспетчерского персонала. – К.: ИПМЭ, 1989. – 53 с.* ***11.*** *Темников В. А., Темникова Е. Л. Определение психофизиологического состояния оператора в системе автоматического внутрисменного мониторинга по голосу // Вестник Восточноукраинского ационального университета им. В. Даля. - №6 (136). – Ч.1. – 2009. – С.294-297.*

Сергей Малышкин
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

УДК 654.924

ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ УГРОЗЫ ИНТЕГРИРОВАННОЙ СИСТЕМОЙ БЕЗОПАСНОСТИ

Аннотация: **Рассматривается модель объекта как совокупность множеств подсистем, угроз объекту и зон объекта. Анализируется суммарная вероятность обнаружения произвольной угрозы интегрированной системой безопасности с учетом вклада подсистем и зон объекта в обнаружение. Анализируется вероятность обнаружения нарушителя с учетом маршрута его проникновения.**
Summary: **The object model is considered as aggregate of a set of the subsystems, the threats and the zones. The total detection probability of a threat by the integrated security system is analyzed with regard to the contribution of the subsystems and the object zones to the detection. The intruder detection probability is analyzed with regard to their penetration route.**
Ключевые слова: **Система безопасности, вероятность обнаружения, угроза.**

I Введение

В настоящее время большое распространение получили интегрированные системы безопасности (ИСБ), подсистемы которых объединены каналами связи и имеют общие средства сбора и обработки информации и управления. Как основные достоинства таких систем обычно отмечаются повышение эффективности управления и сбора информации, проверка тревог (т. е. снижение вероятности ложных тревог) и др. И в меньшей степени учитывается возможность повышения вероятности обнаружения угроз за счет правильной организации взаимодействия (т. е. интеграции) между подсистемами ИСБ. Вследствие интеграции подсистем на том или ином уровне можно говорить об увеличении вероятности обнаружения (ВО) угроз по сравнению со случаем использования отдельных не взаимосвязанных подсистем. В общем случае вероятность обнаружения угрозы ИСБ в целом зависит от вероятностей обнаружения этой угрозы отдельными подсистемами. А вероятность обнаружения угрозы подсистемой, в свою очередь, зависит от параметров средств обнаружения (СО). Поэтому для анализа эффективности ИСБ в целом необходимо знать вклад отдельных СО в обнаружение угроз и, в частности, несанкционированного проникновения. Этим вопросам в отдельности посвящены ряд работ, например, [1 – 3]. Однако в них не рассматривается вопрос в совокупности с учетом специфики именно ИСБ. Поэтому целесообразно дать оценку вероятности обнаружения угрозы интегрированной системой безопасности с учетом возможности повышения вероятности обнаружения за счет интеграции подсистем ИСБ. Такая оценка может служить одним из критериев эффективности ИСБ.

II Модель объекта

В ИСБ обычно каждая подсистема решает свою конкретную задачу. Однако они могут обнаруживать и другие угрозы. Например, обнаружение возгорания может быть произведено, кроме подсистемы пожарной сигнализации, подсистемами охранной сигнализации (к примеру, пассивными инфракрасными извещателями), а также подсистемой телевизионного наблюдения.

Рассмотрим объект, оборудованный интегрированной СБ, состоящей из N подсистем. Совокупность подсистем обозначим множеством $\mathbf{S} = [S_1, S_2, ..., S_N]$. Пусть имеется J возможных угроз данному объекту. В общем случае это могут быть как несанкционированные действия внешнего нарушителя, так и действия персонала, наносящие ущерб целостности объекта, а также угрозы техногенного и природного характера. Относительно объекта угрозы можно разделить на внешние и внутренние. Каждая подсистема решает задачу обнаружения одной (к примеру, возгорание, несанкционированное проникновение) или, в той или иной степени нескольких различных угроз.

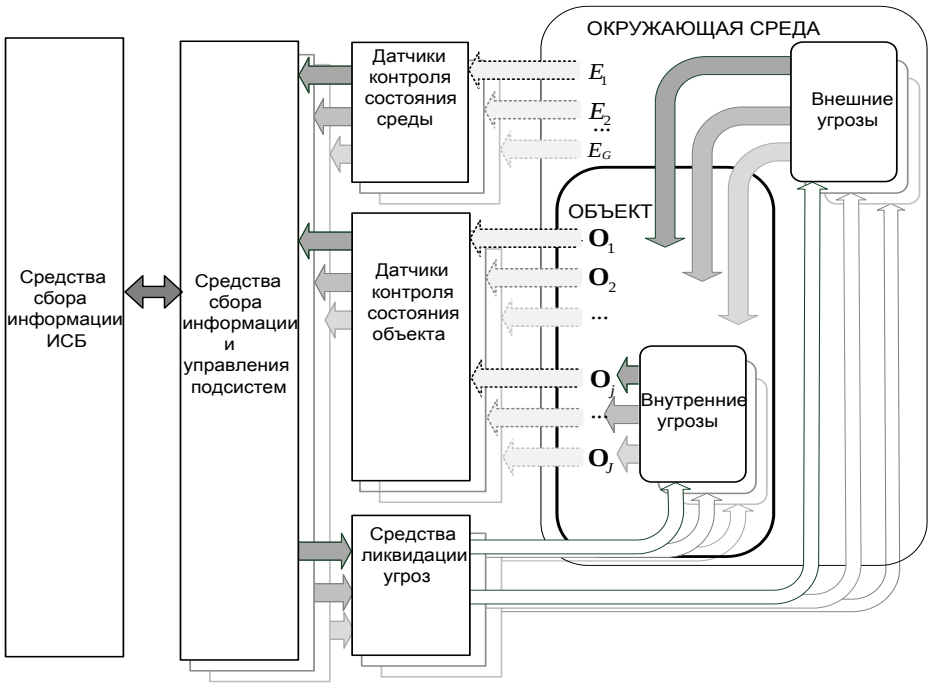

Рисунок 1 – Обобщенная модель системы безопасности

Воспользуемся моделью системы [2], дополнив ее средствами сбора и обработки информации ИСБ (рис. 1). На этой схеме можно выделить множество параметров воздействий окружающей среды $\mathbf{E} = [E_1, E_2, ..., E_G]$, а также множество $\mathbf{O} = [O_1, O_2, ..., O_j, ..., O_J]$, состоящее из J подмножеств, определяющих характер физического проявления той или иной угрозы объекту. Эти множества являются входными воздействиями на систему. Входные воздействия контролируются соответствующими датчиками контроля состояния среды и контроля состояния объекта. Эта информация обрабатывается средствами сбора информации и управления подсистемами. Противодействие угрозам происходит посредством средств ликвидации угроз.

Рассматриваемый объект может быть разделен на I зон обеспечения безопасности. В общем случае многорубежной охраны объект может быть разделен на следующие основные зоны обеспечения безопасности [1]: периметр территории; территория; периметр объекта; внутренний объем; отдельные предметы; система безопасности. А также может быть более детальное деление отдельных зон на дополнительные зоны, в зависимости от решаемых задач.

В зависимости от возможных угроз в каждой зоне располагаются те или иные средства обнаружения угроз, средства инженерной защиты, а также силы реагирования. Множество зон объекта обозначим $\mathbf{Z} = [Z_1, Z_2, ..., Z_I]$. Множества **Z** и **S** образуют соответствие $\mathbf{Q} \subseteq \mathbf{Z} \times \mathbf{S}$. Т. е., в зависимости от решаемых задач та или иная зона может быть оборудована средствами обнаружения одной или нескольких подсистем

ИСБ или ни одной из них. Соответствие включает в себя все возможные пары элементов множеств **Z** и **S**: $\mathbf{Q} = (\{Z_1, S_1\}, \{Z_1, S_2\}, ...\{Z_i, S_n\}, ..., \{Z_I, S_N\})$. Наличие элемента множества $\{Z_i, S_n\}$ обозначает, что *i*-я зона оборудована СО *n*-й подсистемы.

Одной из важнейших характеристик СБ является вероятность P_{nj}^{O} обнаружения *j*-й угрозы *n*-й подсистемой. Понятно, что для разных подсистем возможность обнаружения одной и той же угрозы может быть различной, в зависимости от структуры [3] и выбора параметров СО [4]. В предельных случаях, если *n*-я подсистема не способна обнаружить *j*-ю угрозу, $P_{nj}^{O} = 0$, а если *n*-я подсистема уверенно обнаруживает угрозу, $P_{nj}^{O} \to 1$ [5]. Вероятности обнаружения различными подсистемами различных угроз могут быть представлены в виде матрицы $\mathbf{P^O} = \begin{bmatrix} P_{11}^{O} & ... & P_{1J}^{O} \\ ... & P_{nj}^{O} & ... \\ P_{N1}^{O} & ... & P_{NJ}^{O} \end{bmatrix}$.

Различные угрозы характеризуются вероятностью реализации $P_j^{реал}$ каждой из них, а также условным ущербом $У_j^{H}$, наносимым объекту обеспечения безопасности (ООБ) при их реализации. Это важно учитывать при анализе эффективности СБ, в частности, при оценке предотвращенного ущерба. В общем случае относительный предотвращенный ущерб находится по формуле [1]:

$$У_{П} = B \cdot \prod_{j=1}^{J} P_{jT}^{реал} \left[1 - У_j^{H} \prod_{n=1}^{N} (1 - P_{nj}^{П}) \right],$$

где *B* – важность объекта в относительных единицах, $P_{jT}^{реал}$ – вероятность реализации той или иной угрозы за интервал времени *T*, $У_j^{H}$ – максимальный относительный ущерб, наносимый *j*-й угрозой, $P_{nj}^{П}$ – вероятность предотвращения *n*-й подсистемой безопасности *j*-й угрозы. Последняя связана с вероятностью P_{nj}^{O} следующим соотношением [3]: $P_{nj}^{П} = P_{nj}^{O} \cdot P^{C} \cdot P^{Л}$ где P^{C} – вероятность получения сообщения силами реагирования, $P^{Л}$ – вероятность ликвидации угрозы.

III Вероятность обнаружения угрозы в одной зоне

Рассмотрим частный случай с одной зоной (*I*=1), оборудованной СО нескольких подсистем, способными обнаруживать одну и ту же *j*-ю угрозу с вероятностями $P_{1j}^{O} ... P_{Nj}^{O}$.

Поскольку *j*-я угроза может быть обнаружена несколькими подсистемами, то можно характеризовать вероятность ее обнаружения результирующей вероятностью P_j^{OP}. Оценим результирующую вероятность обнаружения *j*-й угрозы с учетом всех подсистем. Так как различные подсистемы, как правило, используют для обнаружения разные физические принципы, будем исходить из предположения, что вероятность обнаружения угрозы *n*-й подсистемой P_{nj}^{O} не зависит от вероятности обнаружения той же угрозы другими подсистемами. Т. е. в данном случае можно говорить о независимости обнаружения любой из подсистем. Т. о., согласно [8], рассматриваются *N* независимых событий обнаружения *j*-й угрозы *n*-й подсистемой. В этом случае вероятность обнаружения хотя бы одной подсистемой *j*-й угрозы в рассматриваемой зоне P_j^{OP} будет равна:

$$P_j^{OP} = 1 - \prod_{n=1}^{N} (1 - P_{nj}^{O}). \quad (1)$$

Учитывая вероятности обнаружения всех возможных в данной зоне угроз, можно представить их в виде строки матрицы $\mathbf{P^{OP}} = \begin{pmatrix} P_1^{OP} & P_2^{OP} & ... & P_J^{OP} \end{pmatrix}$, где каждый из элементов определяется выражением (1).

IV Вероятность обнаружения угроз на объекте

Обобщим полученное выше выражение (1) с учетом наличия на объекте *I* зон обеспечения безопасности. Каждая из них может характеризоваться результирующей вероятностью обнаружения *j*-й угрозы P_{ij}^{O}. Как было показано выше, *i*-я ЗО характеризуется строкой матрицы вероятностей обнаружения возможных угроз. Компонент матрицы – это результирующая вероятность обнаружения *j*-й угрозы в *i*-й зоне всеми *N* подсистемами.

Таким образом, для всего объекта имеем матрицу обнаружения размерностью $I \times J$:

$\mathbf{P^O} = \begin{bmatrix} P_{11}^{O} & \dots & P_{1J}^{O} \\ \dots & P_{ij}^{O} & \dots \\ P_{I1}^{O} & \dots & P_{IJ}^{O} \end{bmatrix}$, в которой каждому элементу соответствует выражение (1) в *i*-й зоне для *j*-й угрозы.

Кроме того, каждая *j*-я угроза характеризуется своей вероятностью реализации. Обозначим $P_{ij}^{реал}$ как вероятность реализации *j*-й угрозы в *i*-й зоне. Для всего объекта также можно составить матрицу вероятностей реализации угроз: $\mathbf{P}^{реал} = \begin{bmatrix} P_{11}^{реал} & \dots & P_{1J}^{реал} \\ \dots & P_{ij}^{реал} & \dots \\ P_{I1}^{реал} & \dots & P_{IJ}^{реал} \end{bmatrix}$.

Чтобы оценить результирующую вероятность обнаружения P_{j}^{OP} *j*-й угрозы на объекте с учетом различных вероятностей реализации $P_{ij}^{реал}$ *j*-й угрозы в *i*-й зоне в разных зонах, воспользуемся формулой полной вероятности [4]:

$$P_j^{OP} = \sum_{i=1}^{I} P_{ij}^{O} \cdot P_{ij}^{реал} \qquad (2)$$

Выражение под знаком суммы назовем условной вероятностью обнаружения *j*-й угрозы в *i*-й зоне (при условии реализации угрозы). В формуле учитывается вклад каждой ЗО в результирующее обнаружение с учетом вероятности обнаружения и вероятности реализации угрозы. Т. о., если данная угроза маловероятна в той или иной ЗО, т. е. $P_{ij}^{реал} \to 0$, то условная вероятность обнаружения этой угрозы в данной ЗО не сильно скажется на общей сумме.

В результате получаем матрицу результирующей вероятности обнаружения различных угроз на объекте $\mathbf{P^{OP}} = \begin{pmatrix} P_1^{OP} & P_2^{OP} & \dots & P_J^{OP} \end{pmatrix}$. Этот же результат можно получить, произведя частичное умножение матриц $\mathbf{P^O}$ и $\mathbf{P}^{реал^T}$:

$\mathbf{P}_{сумм}^{O} = \mathbf{P}^{O} \times \mathbf{P}^{реал^T} = \begin{bmatrix} P_{11}^{O} & \dots & P_{1J}^{O} \\ \dots & P_{ij}^{O} & \dots \\ P_{I1}^{O} & \dots & P_{IJ}^{O} \end{bmatrix} \times \begin{bmatrix} P_{11}^{реал} & \dots & P_{J1}^{реал} \\ \dots & P_{ji}^{реал} & \dots \\ P_{1I}^{реал} & \dots & P_{JI}^{реал} \end{bmatrix} = \begin{bmatrix} P_1^{OP} & - & - \\ - & P_j^{OP} & - \\ - & - & P_J^{OP} \end{bmatrix}$, где $\mathbf{P}^{реал^T}$ – транспонированная матрица $\mathbf{P}^{реал}$.

В полученной матрице результирующие вероятности обнаружения угроз расположены на главной диагонали.

V Вероятность обнаружения нарушителя на маршруте проникновения

Рассмотрим как частный случай угрозу несанкционированного проникновения нарушителя на объект. Типичный пример многорубежной охраны представляет собой *I* последовательно расположенных неперекрывающихся ЗО. Нарушитель, передвигаясь по объекту по определенному маршруту, пересекает эти ЗО. Вероятность обнаружения *n*-й подсистемой *j*-й угрозы в *i*-й зоне обозначим P_{inj}^{O}. Множество угроз *J* в данном случае может являться множеством возможных типов нарушителей, например,

неквалифицированный, квалифицированный, профессионал и т. п. Сюда же можно включить различные варианты подготовленности, оснащенности, информированности нарушителя, а также их возможные комбинации.

Для представления маршрута НП воспользуемся методом, предложенным в [5].

Определенная конечная чередующаяся последовательность переходов $R_m = \{c_1, c_2, ..., c_l\}$ представляет собой маршрут НП [5]. Маршрут R_m включает в себя подмножество $\mathbf{C}_m \subseteq \mathbf{C}$ множества возможных переходов **C**. Общая продолжительность маршрута T_{R_m} является суммой продолжительностей всех переходов c_m данного маршрута: $T_{R_m} = \sum_{R_m} T_m$.

Как говорилось выше, объект может быть разделен на *I* зон, множество которых обозначили как $\mathbf{Z} = [Z_1, Z_2, ..., Z_I]$. Однако существуют еще препятствия на пути нарушителя – двери, барьеры и т.п. Множество препятствий обозначим $\mathbf{B} = [B_1, B_2, ..., B_K]$. Нарушитель, передвигаясь по маршруту, может перемещаться из одной зоны в другую, а также преодолевать препятствия. При этом элемент маршрута нарушителя – переход – может быть реализован как:

- переход от начала *i*-й зоны до начала *k*-й зоны;
- переход от начала *i*-й зоны до начала *k*-го препятствия;
- преодоление *k*-го препятствия с переходом в *i*-ю зону.

С помощью формулы (1) рассчитываем вероятность обнаружения *j*-й угрозы в *i*-й зоне с учетом N подсистем. Обозначим эту вероятность P_{ij}^O.

Обнаружение нарушителя в той или иной ЗО происходит независимо от обнаружения его в других ЗО, т. е. можно говорить о независимости обнаружения нарушителя каждым из рубежей. Тогда вероятность обнаружения нарушителя хотя бы в одной ЗО рассчитывается по формуле:

$$P_j^O = 1 - \prod_{i=1}^{I}(1 - P_{ij}^O) = 1 - \prod_{i=1}^{I}\left(1 - \left(1 - \prod_{n=1}^{N}(1 - P_{inj}^O)\right)\right) = 1 - \prod_{i=1}^{I}\prod_{n=1}^{N}(1 - P_{inj}^O) \quad (3)$$

При этом суммирование нужно производить только по тем ЗО, которые расположены на маршруте нарушителя. Однако, как известно, в случае угрозы НСД, само по себе обнаружение еще не гарантирует пресечение действий нарушителя, т. е. ликвидацию угрозы. Обнаружение должно быть своевременным, т. е. когда у сил реагирования еще достаточно времени для пресечения НСД. Т.о. при анализе вероятности предотвращения системой безопасности *j*-й угрозы необходим учет временных параметров проникновения, в частности, продолжительностей преодоления препятствий и переходов через зоны. Для этого требуется анализ возможных маршрутов нарушителя.

Говоря о своевременном обнаружении нарушителя необходимо упомянуть такой параметр СБ, как задержка прибытия сил реагирования $T_З$. В соответствии с [1], задержка прибытия сил реагирования слагается из таких составляющих, как время, необходимое для обнаружения НСД СО *i*-й зоны от момента начала воздействия на контролируемый параметр, задержка на формирование сигнала тревоги системой ОС (при проникновении через зоны входа/выхода), длительность передачи извещения системой передачи извещения, задержка на оповещение и продолжительность прибытия сил реагирования.

Согласно принципу своевременного обнаружения эффективность СБ определяется по суммарной вероятности обнаружения нарушителя в момент (критическая точка обнаружения – КТО), когда у сил реагирования еще достаточно времени для его перехвата [7]. В нашем случае время до критической точки обнаружения можно найти, вычтя задержку прибытия сил реагирования из общей продолжительности маршрута нарушителя: $T_{\text{КТО}} = T_{R_m} - T_З$. Обнаружение после КТО не имеет смысла, т. к силы реагирования уже не успеют перехватить нарушителя.

С учетом вышесказанного перепишем выражение (3):

$$P_{jm}^{CO} = 1 - \prod_{l=1}^{\text{КТО}}\prod_{n=1}^{N}(1 - P_{ljn}^O) \quad (4)$$

где P_{jm}^{CO} – вероятность своевременного обнаружения *j*-го нарушителя на *m*-м маршруте.

Таким образом, проанализировав различные возможные маршруты проникновения и рассчитав по формуле (4) вероятности обнаружения нарушителя на упомянутых маршрутах, получим матрицу

вероятностей обнаружения: $\mathbf{P}_j^{CO} = (P_{j1}^{CO}, P_{j2}^{CO}, ..., P_{jM}^{CO})$, где M – количество возможных маршрутов проникновения нарушителя. Данная матрица может характеризовать эффективность ИСБ в отношении угрозы несанкционированного проникновения. При этом минимальное значение вероятности обнаружения $\min(\mathbf{P}_j^{CO})$ характеризует критический с точки зрения ИСБ маршрут нарушителя [7]. Если это значение вероятности своевременного обнаружения меньше требуемого значения вероятности обнаружения, $\min(\mathbf{P}_j^{CO}) < P_{об}$, повысить его можно путем увеличения количества средств обнаружения или увеличения числа барьеров для увеличения времени, требуемого нарушителем на их преодоление. Таким образом, уже на стадии разработки можно оценить необходимое количество средств обнаружения и барьеров без затрат на экспертные оценки и проведение испытаний. А использование данного подхода в специализированных компьютерных программах может упростить и ускорить такую процедуру оценки.

VI Заключение

В работе получены следующие результаты:

1. Формула расчета вероятности обнаружения угрозы интегрированной СБ с учетом вероятности ее реализации в различных зонах объекта.
2. Выражение для расчета вероятности своевременного обнаружения нарушителя на маршруте проникновения интегрированной СБ.

Список использованной литературы: ***1****. Волхонский В. В., Крупнов А. Г. Особенности разработки структуры средств обнаружения угроз охраняемому объекту // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. – № 4(74). – С. 131-136.* ***2****. Волхонский В. В., Воробьев П. А. Методика оценки вероятности обнаружения несанкционированного проникновения оптикоэлектронным извещателем // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 1(77). – С. 120-123.* ***3.*** *Волхонский В. В. Оптимизация структуры и алгоритмов работы комбинированных средств обнаружения проникновения нарушителя // Вестник Воронежского института МВД России. – 2012. – № 2. – С. 91-97.* ***4.*** *Волхонский В. В. Критерии выбора контролируемых средствами обнаружения параметров в системе безопасности // Приборостроение. – СПб.: – 2013. – № 1. – С. 8-12.* ***5.*** *Волхонский, В. В. Системы охранной сигнализации / В. В. Волхонский – 2-е изд., доп. и перераб. – СПб.: Экополис и культура, 2005. – 204 с.* ***6.*** *Волхонский, В. В. Теоретические и методологические основы функционирования устройств и систем обеспечения комплексной безопасности объектов информатизации [Электронный ресурс] / В. В. Волхонский. – Режим доступа: http://vak1.ed.gov.ru/common//img/uploaded/files/VolkhonskiyVV.pdf – Загл. с экрана. – 15.04.2014.* ***7.*** *Гарсиа М. Л. Проектирование и оценка систем физической защиты / М.Л. Гарсиа ; пер. с англ. под ред. Р. Г. Магауенова. – М.: Изд-во Мир, 2003. – 386 с.* ***8.*** *Вентцель, Е. С. Теория вероятностей и ее инженерные приложения: Учеб. пособие для студ. втузов / Е. С. Вентцель, Л. А. Овчаров. – 3-е изд., перераб. и доп. – М.: Издательский центр «Академия», 2003. – 464 с.*