УДК 006.88:004.422.8:681.518.5

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОЦЕНКИ АНТИТЕРРОРИСТИЧЕСКОЙ И ПРОТИВОКРИМИНАЛЬНОЙ ЗАЩИТЫ ОБЪЕКТОВ

© 2014 Н.В.Корнеев, Ю.В.Колесникова

Поволжский государственный университет сервиса, г. Тольятти

Поступила в редакцию 05.02.2014

В статье рассмотрены принципы категорирования и антитеррористической защиты хозяйствующих объектов, разработан алгоритм категорирования объектов, который устанавливает связь, сообразуясь с полем угроз. Проведен анализ средства обнаружения, принципов функционирования системы защиты, противодействия угрозе проникновения нарушителя в охраняемые помещения. Разработана модель нарушителя антитеррористической защиты объектов. Разработано программное средство для имитации нарушителя антитеррористической защиты объектов с использованием динамического программирования. Приведены результаты экспериментальных исследований программного средства.
Ключевые слова: управление, модель нарушителя, математические методы, алгоритмы, динамическое программирование, антитеррористическая защита.

В последние годы чрезвычайно масштабными стали террористические угрозы. Значительно расширился и качественно изменился круг объектов, ставших потенциально опасными. К изначально опасным объектам некоторых отраслей промышленности и науки добавились аэропорты, объекты массового скопления людей, муниципального управления и самоуправления, ряд других объектов. В сфере “обычной” преступности выросла доля имущественных преступлений.

Многие объекты приобрели формы негосударственной собственности, поэтому рациональное распределение бюджетных средств на решение задач безопасности, при всей заинтересованности государства в защите объектов от терроризма и криминала, стало невозможным.

Таким образом, на современном этапе цель категорирования объектов должна быть скорректирована как “создание системы категорирования, предполагающей дифференциацию требований к системе антитеррористической и противокриминальной защиты объектов, обеспечивающей минимально необходимые и достаточные уровни безопасности объектов в соответствии с их категориями потенциальной опасности, с учётом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен преступными действиями в случае невыполнения требований, предъявляемых к системе антитеррористической и противокриминальной защиты объекта (включая полное отсутствие системы) и/или нарушения условий её эксплуатации”.

Корнеев Николай Владимирович, доктор технических наук, профессор кафедры информационного и электронного сервиса. E-mail: niccyper@mail.ru
Колесникова Юлия Владимировна, аспирант. E-mail: YV.Kolesnikova@vaz.ru

Поэтому вопросом категорирования и антитеррористической защиты подведомственных объектов серьезно занимаются как правоохранительные органы, так и ряд других ведомств.

Для определения категории объекта, как правило, применяют критериальный подход [1-4, 6].

Общий алгоритм категорирования объектов можно представить в виде 4-х последовательных шагов:

- 1-й шаг – в соответствии с критериями определяют виды угроз;
- 2-й шаг – устанавливают размеры физического ущерба (количество пострадавших, площади заражённых (попавших в зону действия ЧС) территорий, время, необходимое на восстановление объекта, и т.п.);
- 3-й шаг – осуществляют пересчёт количественных показателей физического ущерба в стоимостные (денежные);
- 4-й шаг – по видам и размерам ущерба устанавливают категорию объекта.

Анализ существующих ведомственных методик категорирования объектов, а также материалов научных наработок по данному вопросу, показывает, что количество категорий следует устанавливать, сообразуясь с полем угроз.

Угрозы безопасности объектов в общем виде можно подразделить на две большие группы: объективные, не зависящие от человека, и субъективные, вызванные тем или иным видом человеческой деятельности:

- объективные угрозы имеют природное происхождение и вызываются, главным образом, стихийными бедствиями, а также техногенными катастрофами и авариями, связанными с ограниченной надежностью техники и не выходящими за пределы заложенных при проектировании объекта рисков;

- субъективные угрозы объекту создаются неумышленными, вынужденными и умышленными (преднамеренными) действиями человека.

Неумышленные угрозы – угрозы, которые вызываются ошибочной деятельностью персонала объекта: халатностью, невнимательностью, недооценкой важности задач и принципов организации систем защиты объекта, последствий возможных угроз.

Вынужденные угрозы – угрозы, которые носят, как правило, социальный характер и выражаются в массовых выступлениях населения, обращениях к власти, исках в суды, блокировании доступа на объект персонала, саботаже, невыплатах за пользование коммунальными услугами и т. п.

Умышленные угрозы можно разделить на:

- криминальные угрозы, которые вызываются деятельностью, относящейся к сфере "общей" преступности и не имеющей чёткой политической окраски;

- террористические угрозы, которые вызываются террористической деятельностью в отношении объектов.

Неумышленные или вынужденные угрозы также могут инициироваться террористами (устрашение или запугивание, использование человеческих слабостей и т. п.).

На первом этапе используют качественные критерии, то есть определяют вид предполагаемого ущерба от террористической акции.

При проведении категорирования рассматриваются также объекты, характеризующиеся:

- наличием категории по гражданской обороне или режиму секретности;

- наличием в составе объекта взрывопожароопасных или пожароопасных помещений и (или) зданий;

- наличием категории по степени радиационной, химической или биологической опасности;

- численностью персонала свыше 500 человек;

- материальными активами свыше 500 тыс. МРОТ [1-4].

Категории потенциальной опасности объектов должны устанавливаться в зависимости от значимости (важности) объектов для обеспечения интересов общества и государства и с учётом развития негативных последствий террористических действий по пессимистическому сценарию.

На втором этапе категорирования используют количественные критерии, позволяющие с достаточной степенью точности определить размеры предполагаемого ущерба.

Основные характеристики возможного ущерба:

- государственно-политический – ущерб государственно-политической системе, обороноспособности и безопасности государства;

- социальный – нанесение вреда отдельным гражданам, большим слоям населения или обществу в целом;

- финансово-экономический – ущерб финансово-кредитной системе и экономике государства;

- экологический – нанесение вреда природным ресурсам и экосистеме.

В зависимости от тяжести последствий (размера и характера возможного ущерба) угрозы разделяют условно на четыре группы:

- низкой степени опасности – вызывающие местные или локальные чрезвычайные ситуации либо сравнимые с ними иные последствия;

- средней степени опасности – вызывающие территориальные чрезвычайные ситуации либо сравнимые с ними иные последствия;

- высокой степени опасности – вызывающие региональные чрезвычайные ситуации либо сравнимые с ними иные последствия;

- очень высокой степени опасности – вызывающие трансграничные или федеральные чрезвычайные ситуации либо сравнимые с ними или более серьезные иные последствия.

Поэтому предлагается [6] система категорирования, которая подразумевает также четыре категории объектов (хотя ведомства, в ведении или сфере ведения которых находятся определённые объекты, могут устанавливать для них большее либо меньшее количество категорий):

- "0" (высшая степень опасности) – ущерб может приобрести международный или федеральный масштаб;

- "I" (очень высокая степень опасности) – ущерб может приобрести отраслевой или межрегиональный масштаб;

- "II" (высокая степень опасности) – ущерб может приобрести региональный или территориальный (уровня субъекта Федерации) масштаб;

- "III" (средняя степень опасности) – ущерб может приобрести местный (муниципального уровня) или локальный масштаб.

Степень защиты конструктивных элементов объекта зависит также от материалов и конструкций, из которых они изготовлены.

Категорирование объектов проводится с целью группирования объектов по функционально-отраслевым признакам и предназначено для формирования перечней объектов различных категорий опасности.

Степень защиты конструктивных объектов в зависимости от категории объекта, классификация оконных конструкций, дверных конструкций, врезных и накладных замков приведена в [6].

Зависимость устойчивости конструкций по категориям и классам от вида разрушающего воздействия приведена в ГОСТ Р 51242-98.

В соответствии с системой категорирования минимальные требования к системам АТПКЗ

(антитеррористической и противокриминальной защиты) и их составляющим ступенчато (по категориям объектов) дифференцируются от "самых жестких" для объектов высшей категории до "самых мягких" для объектов III категории, образуя четыре класса защиты:

- для объектов высшей категории – класс защиты не ниже 4;
- для объектов AI категории – класс защиты не ниже 3;
- для объектов БII категории – класс защиты не ниже 2;
- для объектов БI категории – класс защиты не ниже 1.

При этом можно практически без изменений использовать руководящие документы и рекомендации МВД России [5], в которых представлены количественные и качественные характеристики средств инженерно-технической (ИТУ) укреплённости [6].

Несмотря на экономическую целесообразность применения "достаточных" систем, по решению руководителя или собственника объект может оборудоваться системой и более высокого класса защиты (т. е. "избыточной" системой защиты) – предлагаемая система категорирования этого не запрещает.

Требования по защите дверных и оконных проемов, включая замки, касаются всех зданий, технологических и служебных помещений объекта, за исключением вспомогательных.

Требования к средствам локализации и обезвреживания взрывных устройств, а также индивидуальным средствам защиты – согласно декларации производителя данных изделий и с учётом характера возможных негативных последствий от угроз.

Мотивами нарушений могут быть случайный или спонтанный интерес, причинение ущерба без мотивации (вандализм), хищение имущества, нанесение умышленного вреда людям или имуществу (месть уволенных сотрудников), сбор информации об объекте, диверсия и т.д. В соответствии с целями злоумышленники готовятся к преодолению рубежа охраны, стараясь по возможности остаться незамеченными. При этом знание физического принципа работы, места установки или вида средства обнаружения (СО) облегчает подготовленным нарушителям задачу преодоления зоны охраны (ЗО) без выработки тревоги – в обход. Любой тип СО в той или иной степени уязвим к обходу. Обычно при описании СО не упоминаются возможности обхода. Степень осведомлённости нарушителей о системе охраны различна – от незнания или некоторого знакомства до полного знания и тренированности преодоления.

Метод динамического программирования является оптимальным алгоритмом решения задач исследования процессов в модели нарушителя.

Модели, описывающие поведение людей, активно используются в исследовании операций. Под исследованием операций понимается применение математических, количественных методов для обоснования решений во всех областях целенаправленной человеческой деятельности [8].

Чем сложнее объект, тем большее число переменных характеризует его состояние. Принято называть такой набор переменных вектором состояния объекта и записывать его в виде:

$$\overline{X} = \begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_n \end{vmatrix},$$

где $\overline{X}$ – n-мерный вектор состояния объекта с проекциями x_i; $i = [1, n]$; n – размерность объекта (пространства его состояния).

Можно рассматривать проекции x_i, как координаты некоторого n-мерного пространства, названного для краткости пространством состояний объекта. В этом пространстве по аналогии с трехмерным легко представить переход объекта в новое состояние просто как изменение положения объекта.

Одной из наиболее наглядных (еще важнее – системной) форм описания движения объекта управления является так называемая система дифференциальных уравнений Коши:

$$d\overline{\mathbf{X}} / dt = \Phi(\overline{\mathbf{X}}, \overline{\mathbf{U}}, \overline{\mathbf{F}}, t), \qquad (1)$$

где $\overline{\mathbf{U}}$ – вектор управляющих воздействий размерностью $m \le n$; $\overline{\mathbf{F}}$ – вектор возмущающих воздействий размерностью r, которая не зависит ни от n, ни от m – число внешних возмущений:

$$\overline{\mathbf{U}} = \begin{vmatrix} u_1 \\ u_2 \\ \dots \\ u_m \end{vmatrix}; \quad \overline{\mathbf{F}} = \begin{vmatrix} f_1 \\ f_2 \\ \dots \\ f_r \end{vmatrix},$$

t – аргумент, в качестве которого обычно рассматривается время.

Выражение (1) имеет точный физический смысл – скорость изменения состояния объекта полностью определяется текущим его состоянием (вектором X) и воздействиями, приложенными к объекту.

Формулу (1) называют векторно-матричной, по существу это сокращенная форма записи диф-

ференциальных уравнений движения объекта (изменения состояния объекта). Объекты и устройства управления составляют систему управления, а для рассматриваемой нами задачи:

$$x_k = \varphi_k(x_{k-1}, u_k), \quad k = \overline{1, n},$$

где φ_k – функция перехода.

Управляющее воздействие $U(t)$ на объект этой системы должно обеспечить необходимое движение (изменение состояния) объекта в виде: $X(t) = Z(t)$, где в случае рассматриваемой задачи:

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k), \qquad (2)$$

$f_k(x_{k-1}, u_k) = Z_k$ – показатель эффективности шага k. В рассматриваемом случае состояние x_k на k-ом шаге зависит только от x_{k-1} и управления на k-ом шаге u_k и не зависит от последующих состояний, а также управляющего воздействия.

Таким образом, задача формулируется как определение такого управления $\overline{\mathbf{U}}$, которое переведет систему из начального состояния в конечное, при котором целевая функция (2) принимает оптимальное значение.

Рассмотрим пример реализации предложенного подхода. Объектом анализа является торговая точка, занимающая первый этаж жилого здания. Архитектура анализируемого объекта представлена на рис. 1, где выделены возможные точки входа через внешний периметр и конечные цели, барьеры на пути к целям.

Данный объект, Торговый Дом “СОБИ”, оборудован специалистами фирмы ЗАО “Амулет” с применением программного комплекса САПР СИТЗО “Амулет”.

Возможные точки входа через внешний периметр: 1 – вход через продуктовый магазин; 2 – вход через комнату охраны; 3 – вход №1; 4 – вход №2; 5 – главный вход; 6 – служебный вход; окна. Конечные цели: генеральный директор (зона 7); бухгалтерия (зона 8); администрация (зона 9); банк (зона 10); продуктовый магазин (зона 11); аптека (зона 12).

Барьеры на пути к целям (по сложности): двери между отделами магазинами; главный вход; вход через продуктовый магазин, вход №1, вход №2; двери для персонала; вход через комнату охраны; служебный вход; дверь между отделом для покупателей и служебным помещением, дверь на входе в банк; окна.

Для создания модели нарушителя рассматриваются 3 категории нарушителя:

1. Нарушитель первой категории – специалист с профессиональным образованием с террористическими или иными криминальными намерениями, имеющий дополнительное профессиональное образование по направлению “информационная безопасность”, практический опыт работы по направлению “информационная безопасность” не менее 7 лет, средства преодоления систем защиты объектов

2. Нарушитель второй категории – специалист с профессиональным образованием с террористическими или иными криминальными намерениями, имеющий практический опыт работы по направлению “информационная безопасность” не менее 3 лет.

3. Нарушитель третьей категории – нарушитель без террористических или иных криминальных намерений, основной причиной его нападения на объект является любопытство или личные мотивы.

4. Нарушитель четвертой категории – нарушитель без террористических или иных кри-

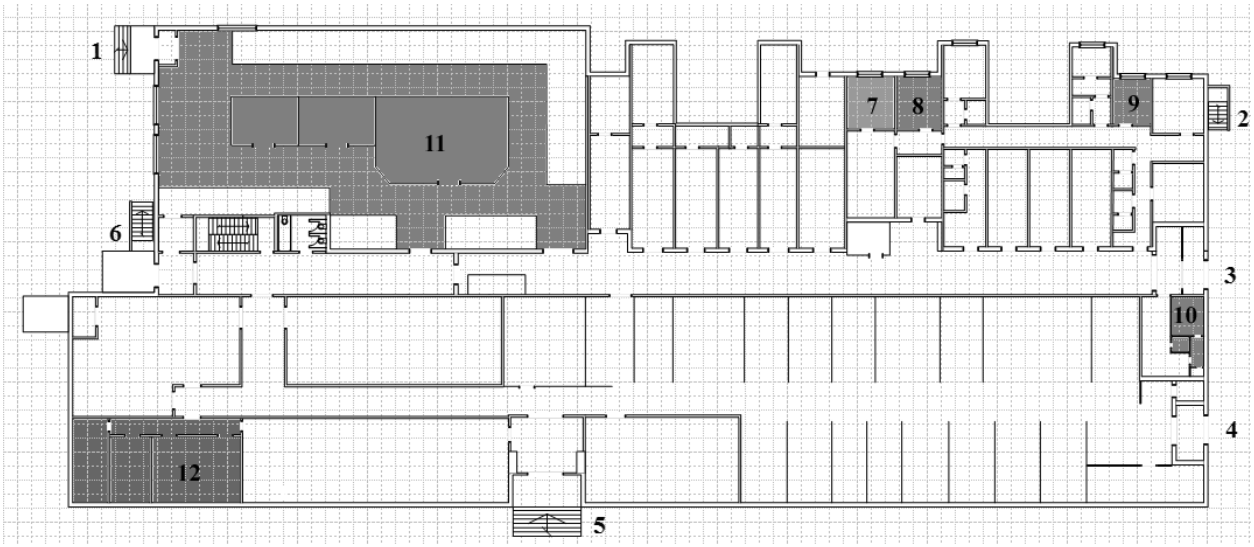

Рис. 1. Архитектура анализируемого объекта, возможные точки входа через внешний периметр и конечные цели

Таблица 1. Соотношение целей между собой

	Генеральный директор	Бухгалтерия	Администрация	Банк	Продуктовый магазин	Аптека
Генеральный директор	-	1	2	3	4	5
Бухгалтерия	-	-	1	2	3	4
Администрация	-	-	-	1	2	3
Банк	-	-	-	-	1	2
Продуктовый магазин	-	-	-	-	-	1
Аптека	-	-	-	-	-	-

Таблица 2. Модель угроз

	Нарушитель 1 категории	Нарушитель 2 категории	Нарушитель 3 категории
Двери между отделами магазинами	1	3	5
Главный вход	1	4	6
Вход через продуктовый магазин, Вход №1, Вход №2	1	5	7
Двери для персонала	2	6	8
Вход через комнату охраны	3	8	10
Служебный вход	3	9	10
Дверь на входе в банк, Дверь между отделом для покупателей и служебным помещением	4	10	-
Окна	10	-	-

минальных намерений, основной причиной его нападения на объект является случайное нахождение в рассматриваемой зоне объекта.

По степени важности и показателям при материальном ущербе цели объекта находятся в соотношениях между собой, представленных в табл. 1.

На основе изложенного выше создадим модель угроз (табл. 2). “Стоимость” преодоления барьера оценивается по 10-балльной шкале. Под “Стоимостью” преодоления барьера подразумевается время, которое потребуется злоумышленнику. Отсутствующая “стоимость” преодоления барьера говорит о невозможности определённого типа злоумышленника преодолеть барьер.

Такие способы преодоления, как разбитие окна, витрины, остеклённой двери или других остеклённых проёмов, взлом двери и другие способы проникновения путём разрушения ограждений, по времени быстрее “тихих” способов проникновения, связанных с применением специальных технических средств (подбор ключей и др.).

Разрушение барьеров влечёт за собой немедленное реагирование службы охраны, и время до момента возможного обнаружения злоумышленника значительно уменьшается, что можно выразить обратно пропорциональным увеличением времени преодоления барьера.

Разработано специальное ПО имитирующее нарушителя, который стремится проникнуть к поставленной цели, преодолев существующие на пути барьеры за минимальное время [7]. Некоторые результаты моделирования маршрута злоумышленника, в зависимости от его цели для цели “Генеральный директор” представлена на рис. 2-4.

Обозначение барьеров на рис. 2-4: 1. Вход через продуктовый магазин; 2. Вход №1; 3. Вход №2; 4. Главный вход; 5. Служебный вход; 6. Вход в комнату охраны; 7. Окна в продуктовый магазин; 8. Окна в кабинет генерального директора; 9. Окна в кабинет бухгалтерии; 10. Окно в столовую; 11. Окно в служебный кабинет; 12. Окна в кабинет

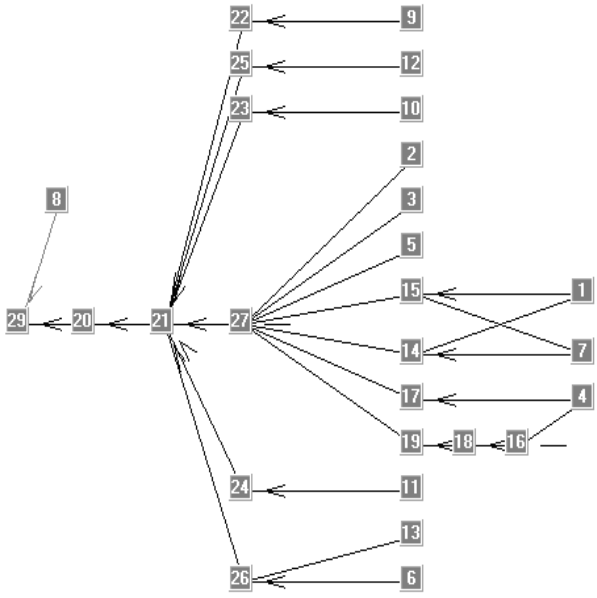

Рис. 2. Граф “Генеральный директор”, пройденный нарушителем 1 категории

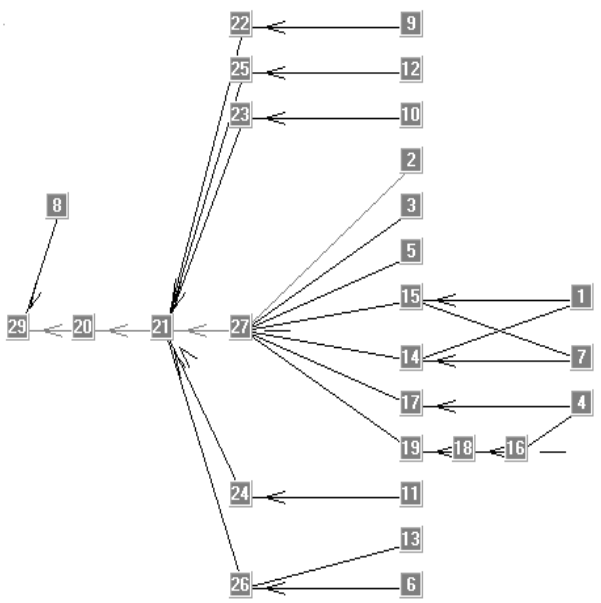

Рис. 3. Граф “Генеральный директор”, пройденный нарушителем 2 категории

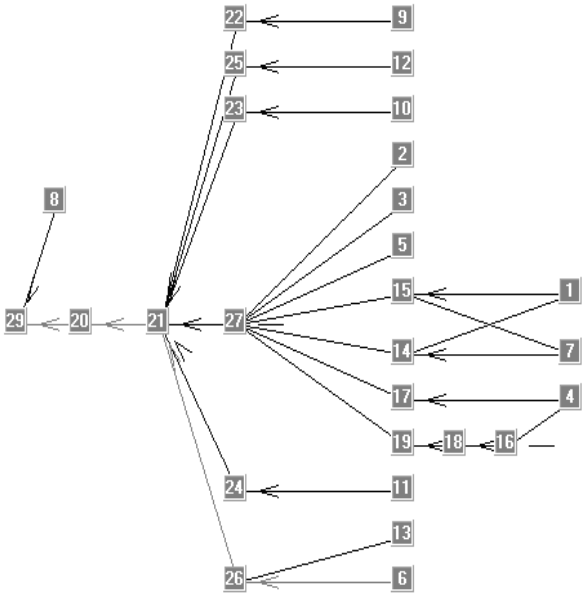

Рис. 4. Граф “Генеральный директор”, пройденный нарушителем 3 категории

администрации; 13. Окно в комнату охраны; 14. Дверь между продуктовым магазином и торг залом для персонала; 15. Дверь между продуктовым магазином и торговым залом; 16. Дверь между аптекой и главным входом; 17. Дверь между аптекой и торговым центром; 18. Дверь в подсобное помещение аптеки для персонала из аптеки; 19. Дверь в подсобное помещение аптеки для персонала из торгового зала; 20. Дверь между кабинетом и приёмной генерального директора; 21. Дверь в приёмную генерального директора; 22. Дверь в кабинет бухгалтерии; 23. Дверь в столовую; 24. Дверь в служебный кабинет; 25. Дверь в кабинет администрации; 26. Дверь в комнату охраны; 27. Дверь между отделом для покупателей и служебным помещением; 28. Дверь на входе в банк.

На рис. 2-4 показаны отдельные графы каждой цели и каждого пути преодоления барьеров каждым нарушителем, а также барьеры, наиболее “привлекательные” для нарушителей по итогам реализованного метода динамического программирования. Рёбра между вершинами на графе соответствуют возможным путям до целей объекта.

ВЫВОДЫ

1. При анализе состояния системы инженерно-технической защиты объекта должны учитываться следующие факторы:

- недостатки нормативных правовых документов по обеспечению безопасности объекта (положение о службе безопасности объекта, должностные инструкции по обеспечению безопасности объекта и т.п.);
- недостаточная степень укомплектованности служб системы обеспечения безопасности объекта (СОБО);
- недостаточная степень квалификации персонала объекта и СОБО;
- наличие сотрудников объекта и СОБО, по тем или иным причинам склонных и способных к противоправным действиям;
- низкий уровень производственной дисциплины персонала объекта и СОБО;
- особенности характеристик объекта (район расположения, топология, состав конструктивных элементов и т.п.);
- особенности технологических процессов, реализуемых на объекте, наличие на нём легко воспламеняющихся и взрывоопасных материалов;
- особенности климатических и природных условий, рельефа в районе расположения объекта и т.п.;
- наличие граничной инфраструктуры (автомобильных/железных дорог);
- большая величина потока посетителей на объекте;
- недостатки инженерно-технических средств системы СОБО;
- наличие уязвимых мест и путей проникновения нарушителей на территорию объекта;
- наличие на объекте потенциально опасного уязвимого элемента, известного нарушителям;
- недостатки системы информационной безопасности объекта;
- ненадлежащее состояние периметра контролируемой зоны объекта;
- наличие значительного количества обслуживающего персонала объекта;

- отсутствие эффективного оперативного контроля за обеспечением безопасности объекта;

- возможность доступа нарушителей к планам объекта;

- доступность средств быстрого распространения опасных веществ (вентиляция, продукты питания и т.п.).

2. Стабильное функционирование системы защиты обеспечивается при комплексном использовании всех видов защиты и координированных действиях сил службы охраны по сигналам, которые формируются техническими средствами охранной сигнализации.

3. Эффективное противодействие проникновению нарушителя на объект возможно путем проведения комплексного анализа включающего совокупности количественных и качественных характеристик вероятного нарушителя. Наиболее эффективны средства охраны (СО), физический принцип действия и способ обхода которых нарушитель не знает. В том случае, когда нарушитель не знает физического принципа действия СО, вероятность обнаружения средства защиты приближается к единице.

4. Разработано специальное ПО имитирующее нарушителя, который стремится проникнуть к поставленной цели, преодолев существующие на пути барьеры за минимальное время. Задача решена методом динамического программирования модели нарушителя антитеррористической и противокриминальной защиты и состояла в выборе оптимальной стратегии нарушителя. Решение задачи позволяет представить поведение злоумышленника, что облегчает создание оптимальной системы безопасности с учётом модели реагирования службы безопасности на объекте. При это предполагается, что нарушитель хорошо подготовлен с точки зрения построения математических моделей при расчёте своего маршрута.

5. Эффективность всей системы защиты от несанкционированного проникновения необходимо оценивать по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности.

6. С течением времени необходима модернизация методов и средств защиты, актуализация и пересмотр базы шаблонов динамического программирования модели нарушителя, что должно соответствовать основной концепции безопасности и диверсификации концепции защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Об информации, информационных технологиях и защите информации. Закон РФ от 27.07.2006 г. № 149-ФЗ.
2. Концепция национальной безопасности РФ. Утверждена указом Президента РФ от 17.12.97, № 1300. Российская газета от 26.12.97.
3. О коммерческой тайне. Закон РФ от 29.07.2004 г. № 98-ФЗ.
4. О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств. Приказ Минтранса РФ от 03.11.2009 г. № 194.
5. РТМ-1-2-2-92 Системы безопасности объектов федеральной собственности. Системы охранной безопасности. Категории важности объектов. М.: НИЦ “Охрана” ВНИИПО МВД РФ, 1992. 15 с.
6. *Корнеев Н.В., Колесникова Ю.В.* Категорирование объектов при разработке специального математического и программного обеспечения динамического программирования модели нарушителя антитеррористической и противокриминальной защиты. // Программная инженерия и информационная безопасность. 2013. №2. С. 32...40
7. Свидетельство о государственной регистрации программы для ЭВМ №2013616953, 29.07.13
8. *Вентцель Е.С.* Введение в исследование операций. М.: Советское радио, 1964. 391 с.

SOFTWARE FOR THE ESTIMATION ANTITERRORIST AND AGAINST CRIMINAL GUARDS OF OBJECTS

© 2014 N.V. Korneev, J.V. Kolesnikova

Volga Region State University of Service, Togliatti

In paper sharing principles on a category and an antiterrorist guard of managing objects are considered, the algorithm of sharing on a category of objects which establishs communication is developed, being conformed to the field of threats. The analysis of a sensor, principles of performance of a protection system, bucking to threat of penetration of the infringer in guarded locations is carried out. The model of the infringer of an antiterrorist guard of objects is developed. The software is developed for cloning of the infringer of an antiterrorist guard of objects with dynamic programming usage. Outcomes of experimental researches of a software are reduced.

Key words: handle, model of the infringer, mathematical methods, algorithms, dynamic programming, antiterrorist guard.

Nikolay Korneev, Doctor of Technics., Professor at the Information and Electronic Service Department.
E-mail: niccyper@mail.ru
Julia Kolesnikov, Post-Graduate Student.
E-mail: YV.Kolesnikova@vaz.ru