УДК 006.88:004.422.8

Н.В. Корнеев[1], Ю.В. Колесникова[2]
([1]Поволжский государственный университет сервиса, [2]ОАО "АВТОВАЗ";
e-mail: niccyper@mail.ru)

О ПОСТРОЕНИИ МОДЕЛИ ДЕЙСТВИЙ НАРУШИТЕЛЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ

Проведён анализ средств обнаружения, принципов функционирования системы защиты, противодействия угрозе проникновения нарушителя в охраняемые помещения. Разработана модель поведения нарушителя.

Ключевые слова: управление, модель нарушителя, математические методы, алгоритмы, динамическое программирование, антитеррористическая защита

N.V. Korneyev, J.V. Kolesnikova

ABOUT CONSTRUCTION OF MODEL BEHAVIOR OF INFRINGER OF THE ANTITERRORIST GUARD OF OBJECTS WITH DYNAMIC PROGRAMMING USAGE

The analysis of detection means, principles of performance of a protection system, combating the threat of penetration of the infringer in guarded locations is carried out. The model of the behavior infringer is developed.

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

Статья поступила в редакцию Интернет-журнала 22 марта 2013 г.

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 пребывания людей, муниципального управления и самоуправления, ряд других объектов. В сфере "обычной" преступности выросла доля имущественных преступлений [1].

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 [8].

Таким образом, на современном этапе цель комплексной безопасности организаций 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" [9, 10].

Основные принципы построения указанной системы изложены в [9, 10].

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 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 [2, 3].

Метод динамического программирования является оптимальным для решения задач исследования процессов в модели действий 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 [5].

Представим себе некоторую операцию Q, распадающуюся на ряд последовательных шагов. Некоторые операции расчленяются на шаги естественно, в некоторых членение приходится вводить.

Управляемый процесс выглядит примерно следующим образом. Управление можно разбить на n шагов и решение принимается последовательно на каждом шаге, а управление, переводящее систему из начального состояния в конечное, представляет собой совокупность n пошаговых управлений. В результате управления система переходит из состояния x_0 в x_n.

Обозначим через $u_k \in U_k$ управление на k-м шаге (k = 1, 2, ..., n). U_k – множество допустимых управлений на k-м шаге. Пусть $u = (u_1, u_2, \ldots, u_n)$ – управление, переводящее систему из состояния x_0 в состояние x_n. Обозначим через x_k состояние системы после k-го шага управления. Получается последовательность состояний $x_0, x_1, \ldots, x_{k-1}, x_k, x_{k+1}, \ldots, x_n$, проиллюстрированная на рис. 1.

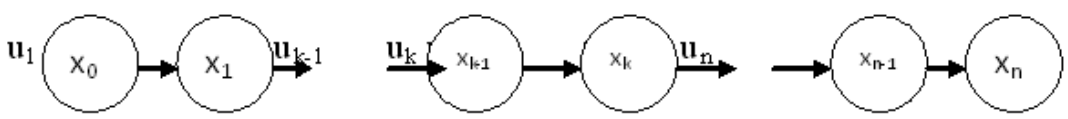

Рис. 1. Переход системы из одного состояния в другое
в результате воздействия управляющих сигналов

Показатель эффективности рассматриваемой управляемой операции зависит от начального состояния и управления:

$$Z = F(x_0, u), \quad (1)$$

где $u \in U$ – множество возможных управлений.

Сделаем несколько предположений:

1. Состояние x_k системы на k-м шаге зависит только от предшествующего состояния x_{k-1} и управления на k-м шаге u_k и не зависит от следующих состояний и управлений (свойство отсутствия последействия):

уравнения состояний:

$$x_k = \varphi_k(x_{k-1}, u_k), \ k = \overline{1, n}, \quad (2)$$

где φ_k – оператор перехода.

2. Целевая функция (1) является аддитивной от показателя эффективности каждого шага, то есть выигрыш за всю операцию складывается из выигрышей на отдельных шагах:

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k), \quad (3)$$

где $f_k(x_{k-1}, u_k) = Z_k$ – показатель эффективности шага k.

Общая постановка задачи динамического программирования: определить такое допустимое управление $u \in U$, переводящее систему из состояния x_0 в состояние x_n, при котором целевая функция (3) принимает оптимальное значение.

Рассмотрим пример реализации предложенного подхода. Объектом анализа является торговая точка, занимающая первый этаж жилого здания. Архитектура анализируемого объекта представлена на рис. 2, где выделены возможные точки входа через внешний периметр и конечные цели: барьеры на пути к целям представлены на рис. 3.

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

Конечные цели: генеральный директор (красная зона); бухгалтерия (жёлтая зона); администрация (зелёная зона); банк (голубая зона); продуктовый магазин (синяя зона); аптека (фиолетовая зона).

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;

7 – окна.

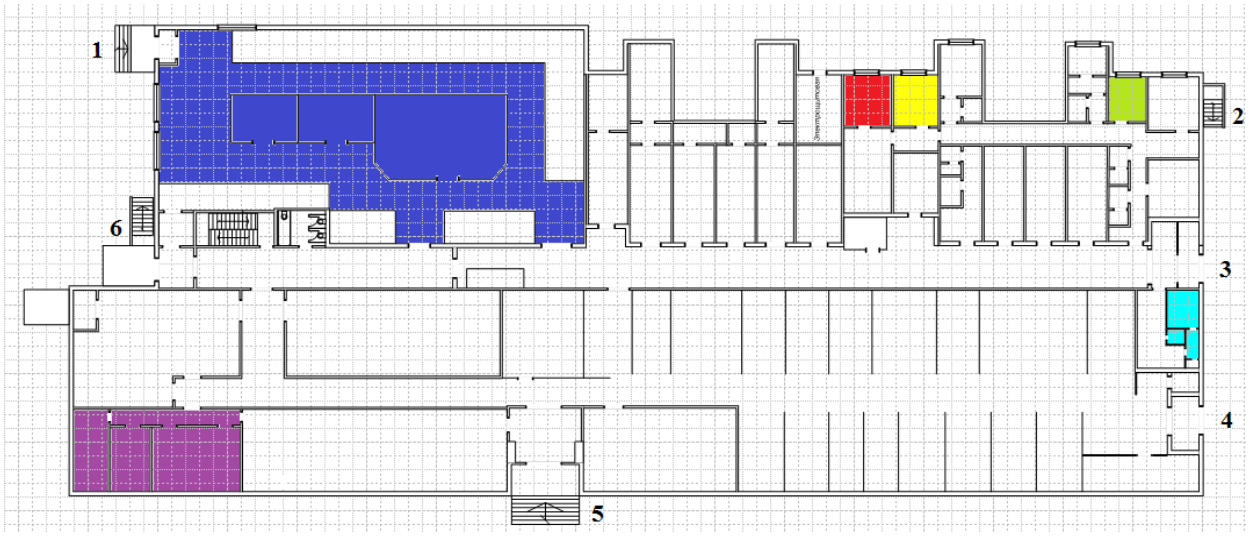

Рис. 2. Возможные точки входа через внешний периметр и конечные цели

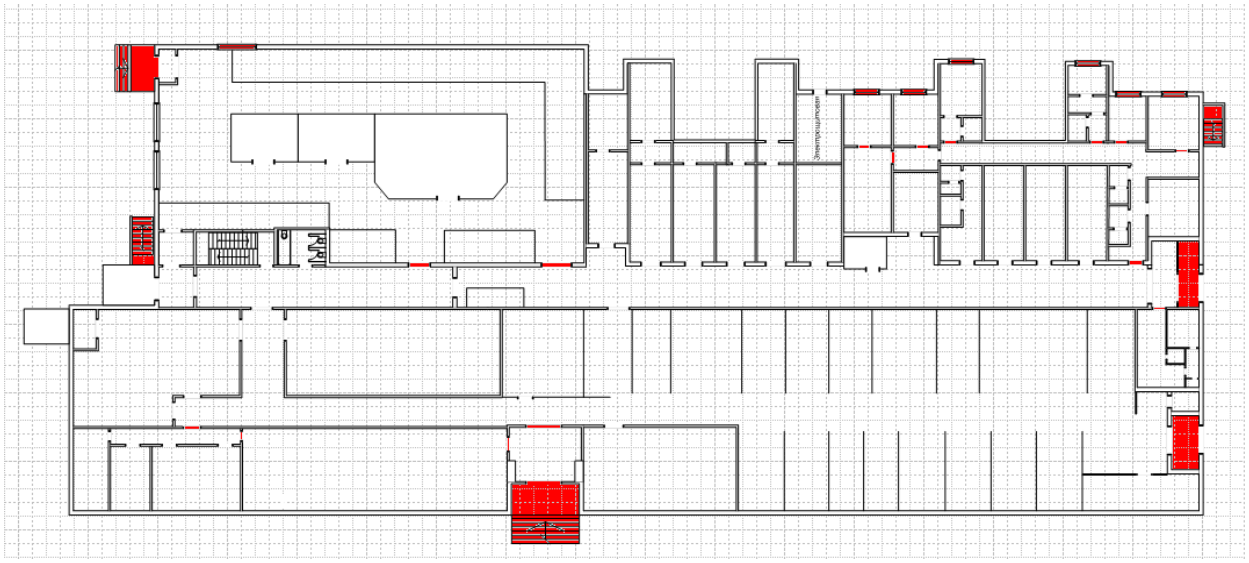

Рис. 3. Барьеры на пути к целям

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 действий нарушителя рассматриваются 4 категории нарушителя:

- нарушитель первой категории – специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

• нарушитель второй категории – непрофессиональный нарушитель с враждебными намерениями, имеющий определённую подготовку для проникновения на конкретный объект;

• нарушитель третьей категории – нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

• нарушитель четвертой категории – нарушитель без враждебных намерений, случайно нарушающий безопасность объекта, не рассматривается в силу трудности предположения поведения на объекте.

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

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	-	-	-	-	-	-

На основе изложенного выше создадим модель угроз (табл. 2).

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	-	-

"Стоимость" преодоления барьера оценивается по 10-балльной шкале. Под "Стоимостью" преодоления барьера подразумевается время, которое потребуется нарушителю. Отсутствующая "стоимость" преодоления барьера говорит о невозможности определённого типа нарушителя 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 нарушителя значительно уменьшается, что можно выразить обратно пропорциональным увеличением времени преодоления барьера.

Моделирование маршрута нарушителя для цели "Генеральный директор" представлена на рис. 4.

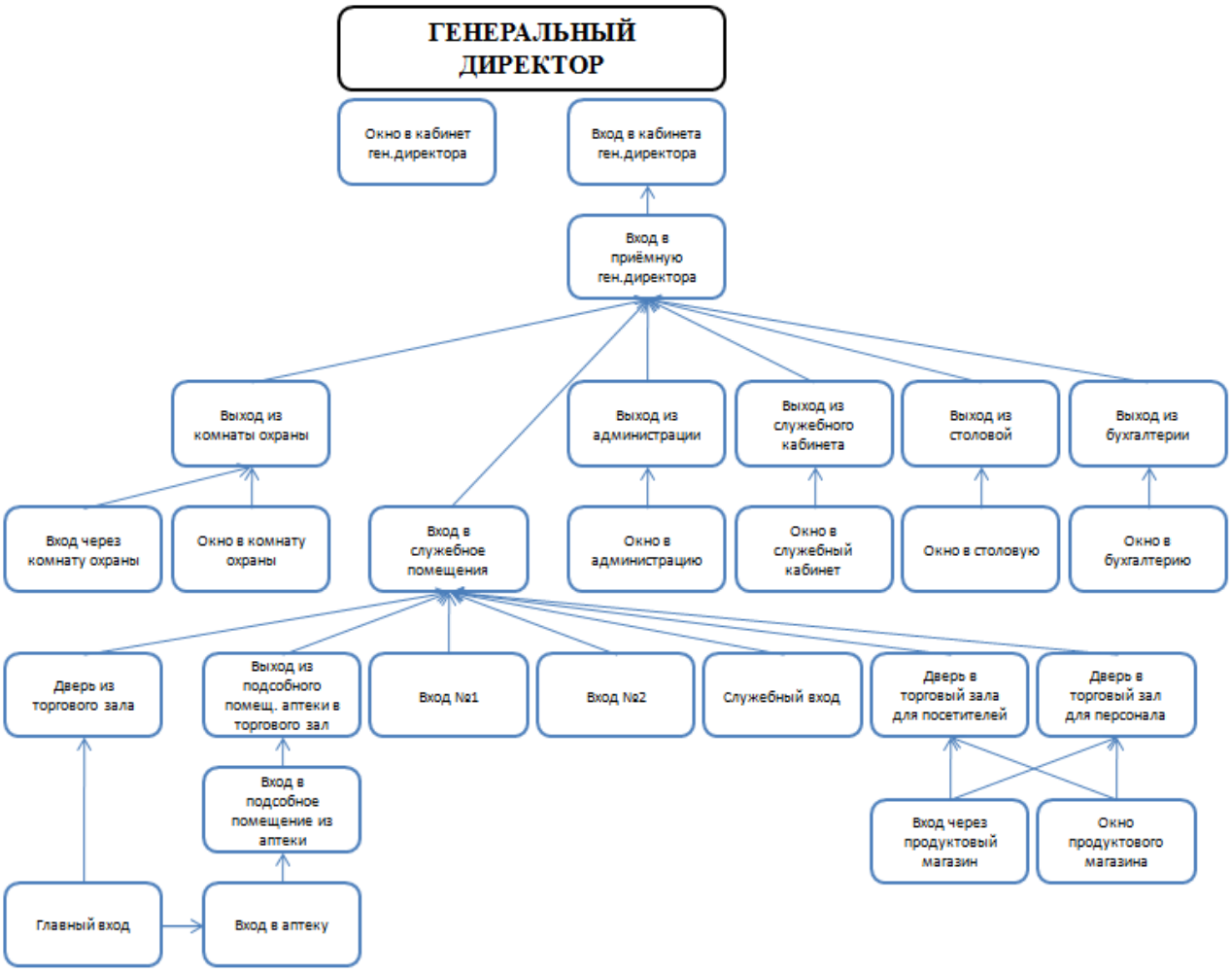

Рис. 4. Барьеры на пути к цели "Генеральный директор"

Отдельные графы каждой цели и каждого пути преодоления барьеров каждым нарушителем, а также барьеры, наиболее "привлекательные" для нарушителей, по итогам реализованного метода динамического программирования, изображены на рис. 5-8.

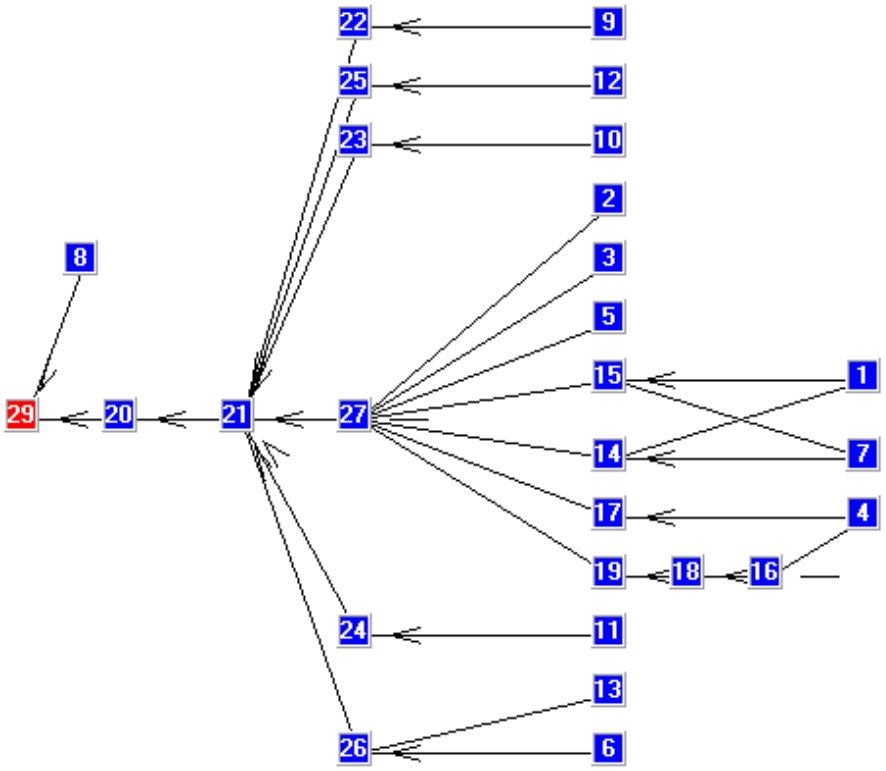

Рис. 5. Граф "Генеральный директор"

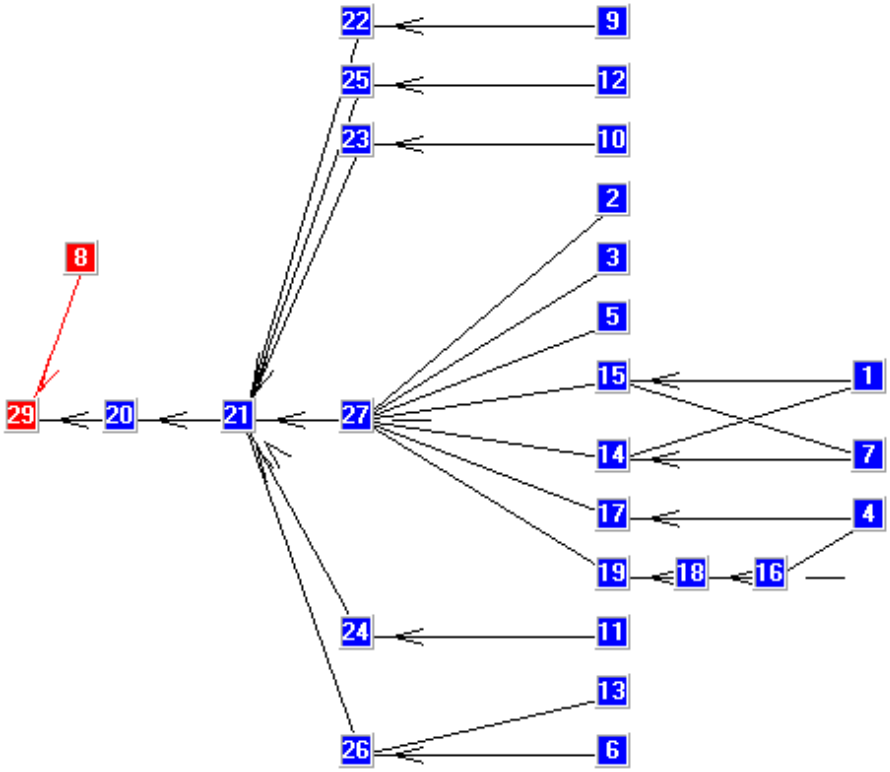

Рис. 6. Граф "Генеральный директор", пройденный нарушителем 1 категории

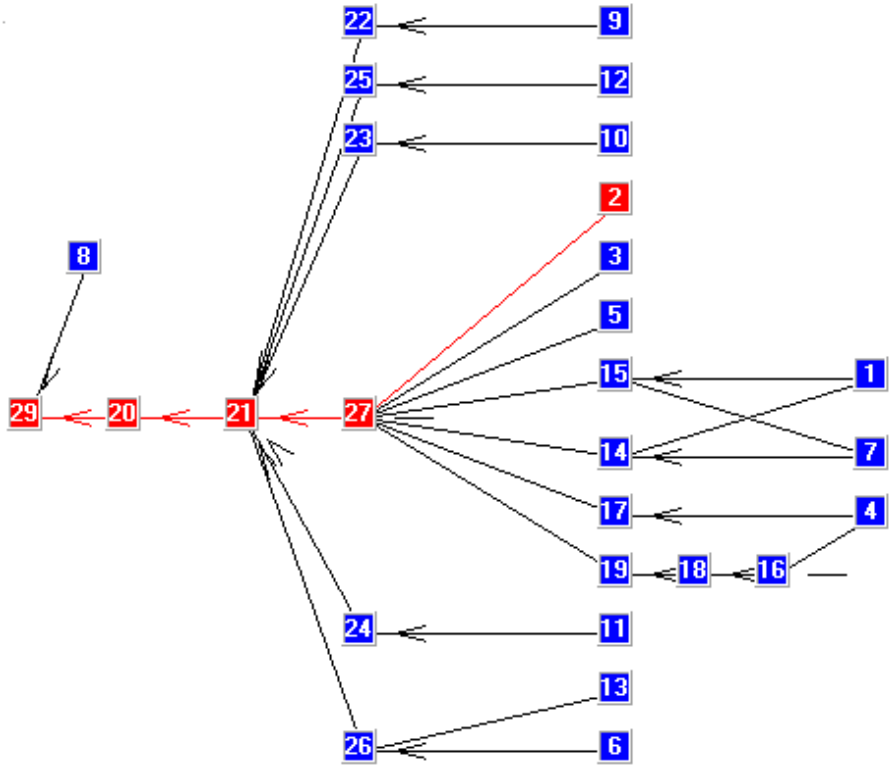

Рис. 7. Граф "Генеральный директор", пройденный нарушителем 2 категории

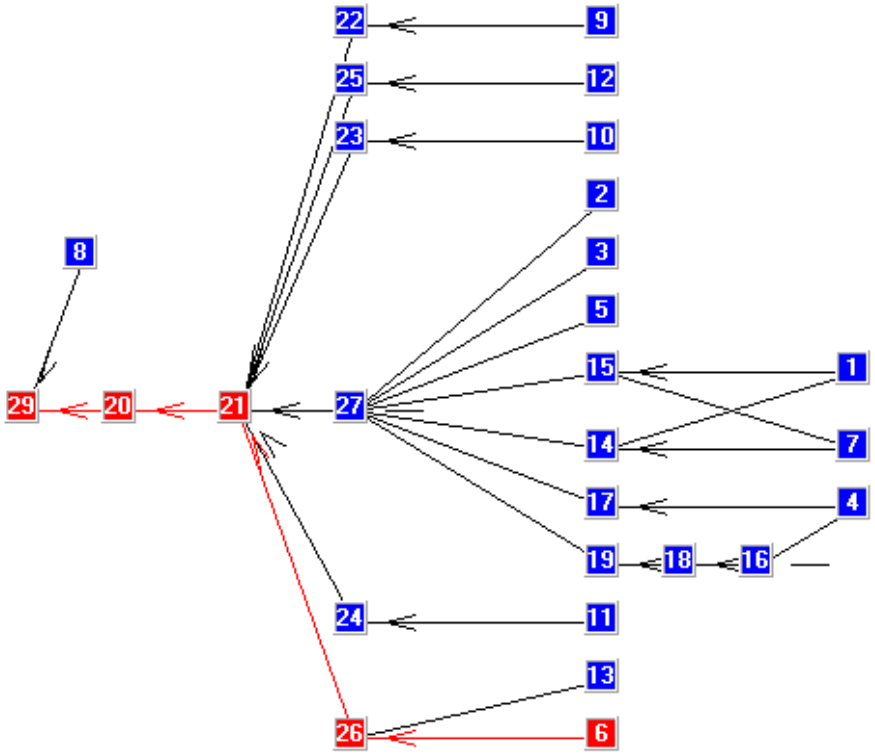

Рис. 8. Граф "Генеральный директор", пройденный нарушителем 3 категории

Обозначение барьеров:

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 администрации;

13 – окно в комнату охраны;

14 – дверь между продуктовым магазином и торговым 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;

29 – кабинет генерального директора.

Рёбра между вершинами на графе соответствуют возможным путям до целей объекта.

Выводы

Стабильное функционирование системы защиты объектов обеспечивается при комплексном использовании всех видов защиты и координированных действиях сил службы охраны по сигналам, которые формируются техническими средствами охранной сигнализации [7].

Эффективное противодействие проникновению нарушителя на объект возможно путём проведения комплексного анализа, включающего совокупности количественных и качественных характеристик вероятного нарушителя.

Наиболее эффективны средства обнаружения, физический принцип действия и способ обхода которых нарушитель не знает.

Полученные авторами результаты могут быть использованы при разработке специального программного обеспечения, имитирующего нарушителя, который стремится проникнуть к поставленной цели, преодолев существующие на пути барьеры за минимальное время. Обобщенная задача решается методом динамического программирования поведения нарушителя антитеррористической и противокриминальной защиты и состоит в выборе оптимальной стратегии нарушителя.

Решение задачи позволяет представить поведение нарушителя, 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.

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

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.

Литература

1. ***Коновалов В.А., Севрюков Д.В., Хасянов Р.С.*** Категорирование объектов. Ключевой фактор обеспечения эффективности систем комплексной безопасности // Системы безопасности. № 6. 2006, 4 с.

2. ***Корнеев Н.В.*** Концептуальные подходы к оснащению современными системами безопасности предприятий социально-культурного сервиса и туризма // Естественные и технические науки. № 3. 2009. 4 с.

3. ***Корнеев Н.В.*** Комплексные системы защиты информации на предприятии: учебно-методическое пособие для выполнения лабораторных работ по дисциплине "Комплексные системы защиты информации на предприятии". М.: Спутник+, 2012. 97 с.

4. ***Корнеев Н.В., Мальцев Н.В.*** Принципы построения модели безопасности инновационного предприятия при вузе с учётом различных особенностей его функционирования // Учёные записки РГСУ. №3. 2012. С. 151-156.

5. ***Корнеев Н.В.*** Принципы разработки современных бесконтактных бесконтактных средств идентификации // Техника машиностроения: научно-технический журнал. № 2 (82). 2012. С. 26-33.

6. ***Корнеев Н.В., Башлыкова А.А.*** Задачи оценки качества программного обеспечения по критериям информационной безопасности // Техника машиностроения: научно-технический журнал. № 3 (83). 2012. С. 19-23.

7. ***Корнеев Н.В., Мальцев Н.В., Смолин С.Л.*** Факторы антропогенного характера дестабилизирующие систему безопасности, как последствия негативного влияния на социум информационного пространства // Учёные записки РГСУ. № 6. 2012. С. 35-41.

8. ***Jeffrey S. Smith, Brett A. Peters, Sabina E. Jordan, Mark K.Snell.*** Распределенное моделирование в реальном времени системного анализа обнаружения нарушителя. Department of Industrial Engineering Texas A&M University College Station, TX 77843, U.S.A. Proceedings of the 1998 Winter Simulation Conference D.J. Medeiros, E.F. Watson, J.S. Carson and M.S. Manivannan, eds.

9. ***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. № 2. 2013. С. 17-23.

10. ***Корнеев Н.В.*** Алгоритмические и программные методы и средства оценки альтернативных проектов защиты системы обработки информации предприятия на основе многокритериального анализа: монография. М.: Изд-во "Спутник+", 2013. 117 с.