

УДК 621.03.9

Е.В. АЗАРЕНКО, Н.А. БОРОДИНА, М.М. ДИВИЗИНЮК,
Н.В. КАСАТКИНА, С.В. ЛАЗАРЕНКО, Е.А. РЫБКА

Государственное предприятие «Институт геохимии окружающей среды НАН Украины»

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫЯВЛЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА С ИСПОЛЬЗОВАНИЕМ ОБРАЗОВ ЛЮДЕЙ, НАХОДЯЩИХСЯ ОКОЛО ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В работе проанализирован порядок описания штатного состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта критической инфраструктуры. Рассмотрена последовательность выявления нештатных ситуаций с лицами, находящимися в контролируемой зоне охраняемого объекта критической инфраструктуры. Определен процесс оптимального приведения состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта, из нештатного состояния в штатное. Полученные зависимости объединены в соответствующую математическую модель.

Ключевые слова: охраняемый объект критической инфраструктуры, лица, находящиеся в контролируемой зоне, ситуационный фон, видеосистема, злоумышленник.

E.V. AZARENKO, N.A. BORODINA, M.M. DIVIZYNIUK,
N.V. KASATKINA, S.V. LAZARENKO, E.A. RYBKA

State Institution «Institute of Environmental Geochemistry of the NAS of Ukraine»

MATHEMATICAL MODEL OF IDENTIFICATION OF NONSTATE SITUATIONS OF A TERRORIST CHARACTER WITH THE USE OF IMAGES OF PEOPLE UNDERLYING OBJECTS OF CRITICAL INFRASTRUCTURE

In this paper, we describe the development of a mathematical model for identifying abnormal situations of a terrorist nature using images of people located near critical infrastructure facilities. This description consists of three stages. Initially, the procedure for describing the staffing status of the situation background of persons in the controlled area of the protected critical infrastructure facility was analyzed. It is shown that the whole multitude of people located near the protected critical infrastructure facility was divided into three categories. The first is the personnel, which ensures the operation of the protected facility, and has access to the main or additional protected areas. Secondly, citizens permanently residing in the controlled zone around the protected facility. These are family members of the personnel of the protected facility. They are citizens and their families, who work at enterprises and firms that serve the city of the satellite. Third - guests and business travelers. Regardless of belonging to one or another category in the database and knowledge of the main server of the protected object for each person who has visited the controlled area, there is an individual form. Two dependencies are given, which show that the chaotic movement of people in the controlled zone depends on the principle attitude to the protected object. The sequence of detection of abnormal situations with persons in the controlled area of the protected critical infrastructure facility is considered. This dependence shows the possibility of fixing contacts of an intruder or an attacker, identified by an operational database. This means that if an intruder or an attacker whose image is present in the operational database will be registered (photographed) by a video system, then he will be identified.

Keywords: A protected critical infrastructure object, persons in the controlled area, a situation background, a video system, an attacker.

Введение

Термин «инфраструктура» означает комплекс взаимно связанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования единой системы [1]. Государственные предприятия и учреждения в своем составе, как правило, имеют специфические инфраструктуры, которые полноценно функционируют при наличии внешних, заграничных связей и обеспечивают инновационную [2, 3], рыночную [4, 5], информационную [6] деятельность. Имеются и другие специфические инфраструктуры, например, военная [7], деятельность которых носит закрытый характер.

В целом на государственном уровне выделяют национальную критическую инфраструктуру, которая определяется как совокупность систем, нарушение деятельности хотя бы одной из которых может нанести серьезный ущерб экономике государства или привести к негативным социальным последствиями в обществе.

Каждая из систем, например, энергетическая, топливная, телекоммуникационная, транспортная, водообеспечения имеют в своей структуре предприятия, относящиеся к критически важным объектам, выход из строя которых может вызвать кризис на общегосударственном, региональном или местном уровне. К таким объектам относятся атомные и гидроэлектростанции, химические и нефтехимические комбинаты, металлургические заводы и множество других государственных и частных предприятий и учреждений стратегического назначения [8-11].

Для обеспечения максимального устрашающего эффекта путем увеличения потерь среди мирного населения, а также с целью привести к экономическим и социальным потерям в отдельном регионе страны или даже государстве в целом, террористы стремятся вывести из строя, прежде всего, критически важные объекты. Поэтому обеспечение их безопасности посредством противодействия террористическим актам является чрезвычайно важной и актуальной научной задачей.

Исходя из специфики протекания чрезвычайной ситуации террористического характера на охраняемом объекте критической инфраструктуры, а также с учетом особенностей управления процессами, вызванными чрезвычайными ситуациями, происходящими в других областях, разработана структурно-логическая модель

управления чрезвычайной ситуацией террористического характера [12]. Она состоит из шести структурных элементов, которым соответствуют конкретные фазы процесса управления. Составные части модели по сути представляют собой методы, способы и организационно-технические мероприятия, направленные на предотвращение чрезвычайной ситуации террористического характера. Это мониторинг ситуации (сбор повседневных факторов), выявление риска (обнаружение экстремального фактора), анализ риска (прогноз и моделирование чрезвычайной ситуации), подготовка вариантов управленческих решений, принятие решения и доведение его исполнителям, воздействие на ситуацию. В совокупности они образуют контур управления и обеспечивают непрерывность процесса управления чрезвычайной ситуацией террористического характера в интересах ее недопущения и предотвращения. Использование при этом видеoinформации о событиях, происходящих в контролируемой зоне около объекта критической инфраструктуры, позволяет в результате сбора повседневных факторов и анализа полученной информации заблаговременно выявлять признаки, предшествующие чрезвычайным ситуациям террористического характера.

Постановка цели и задач научного исследования

Цель данной работы – разработка математической модели выявления нештатных ситуаций террористического характера с использованием образов людей, находящихся около объектов критической инфраструктуры.

Для достижения поставленной цели необходимо решить следующие задачи. Во-первых, проанализировать порядок описания штатного состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта критической инфраструктуры. Во-вторых, рассмотреть последовательность выявления нештатных ситуаций с лицами, находящимися в контролируемой зоне охраняемого объекта критической инфраструктуры. В-третьих, определить процесс оптимального приведения состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта, из нештатного состояния в штатное.

Порядок описания штатного состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта критической инфраструктуры

Рассмотрим совокупность людей, находящихся около охраняемого объекта критической инфраструктуры, и разделим ее условно на три категории, исходя из условия принадлежности к охраняемому объекту. К первой категории относится персонал, который обеспечивает работу предприятия и имеет доступ на основную или дополнительную охраняемые территории. Вторая категория – это граждане, постоянно проживающие в контролируемой зоне вокруг охраняемого объекта – члены семей персонала охраняемого объекта, а также сотрудники предприятий и учреждений, обслуживающих город-спутник, и их семьи. Третья категория – гости и командированные.

Независимо от принадлежности к той или иной категории в базе данных и знаний главного сервера охраняемого объекта на каждого человека, побывавшего в контролируемой зоне, заводится индивидуальный формуляр, в котором содержится пять групп данных: 1) анкетные данные; 2) вне анкетные данные; 3) антропометрические характеристики лица, по которым происходит основное опознавание (идентификация) личности (словесные описания лица и фотографические образы в различных комбинациях, например, в очках, в парике и др.); 4) антропометрические параметры тела и биометрические характеристики (отпечатки пальцев, картина роговицы глаз, особые приметы и т. п.); 5) поведенческие характеристики индивида, а именно: характеристики безусловных поведенческих движений, сохраняющихся в течение всей жизни (походка, ужимки, ухмылки, жесты и пр.), служащие дополнительным средством идентификации при отсутствии фотографии лица, и поведенческие характеристики, связанные с охраняемым объектом, то есть все перемещения и контакты человека вне объекта, если он относится к персоналу. В остальных случаях на индивида, будь то постоянно проживающий в контролируемой зоне или гость, или командированный, собирается и систематизируется вся информация, поступающая от видеосистем наружного наблюдения.

Для исследования закономерностей поведения людей в контролируемой зоне вокруг охраняемого объекта допустим, что их перемещение является хаотическим и аналогично броуновскому хаотическому движению. В результате получено, что поток $j(\Lambda, t)$ людей, находящихся в контролируемой зоне вокруг охраняемого объекта радиусом R , зависит от их положения Λ_0 , которое описывается с помощью d -функций:

$$\begin{cases} j(\Lambda) = \frac{1}{R}, \\ j(\Lambda) = \left(1 - \frac{\Lambda_0}{R}\right) d(\Lambda) + \frac{\Lambda_0}{R} d(\Lambda - R). \end{cases} \quad (1)$$

Соотношения (1) показывают, что хаотическое перемещение людей в контролируемой зоне принципиально зависит от их принадлежности к охраняемому объекту. В соответствии с первым выражением гости или командированные рано или поздно покинут пределы контролируемой зоны, а из второго выражения следует, что персонал и постоянно проживающие в зоне люди ограничивают свои перемещения внутри контролируемой зоны. Если приезжие длительное время не покидают контролируемую зону, значит, они имеют некоторый интерес в отношении охраняемого объекта.

Последовательность выявления нештатных ситуаций с лицами, находящимися в контролируемой зоне охраняемого объекта критической инфраструктуры

Поток лиц, регистрируемый видеосистемами в контролируемой зоне так же, как хаотическое

движение броуновских частиц, является марковским процессом, и для их описания может быть использован соответствующий математический аппарат.

Установлено, что персоналу, постоянно проживающему в контролируемой зоне вокруг охраняемого объекта, гостям и командированным присущи определенные динамические или поведенческие характеристики, которые называются штатными или обычными. Зафиксированная камерами видеонаблюдения информация систематизируется по дням недели, в выходные и праздничные дни, по временам года и позволяет формировать базы данных и знаний о всех лицах, находящихся около объекта критической инфраструктуры, что и определяет ситуационный фон лиц, находящихся около охраняемого объекта. Чем больше видео фиксаций человека будет сделано, тем точнее получается картина его обычного, типового поведения, которая относится к его штатным характеристикам. На основании отклонений в поведении субъекта от штатных характеристик, которые считаются нарушениями, происходит выявление признаков, предшествующих нештатным ситуациям.

Нарушения принято разделять на пять уровней. Отклонения 1-го уровня представляют собой изменения обычного поведения индивида, которые регистрируются (видеофиксация) видеосистемами наружного наблюдения и транслируются в базу данных и знаний, где происходит их систематизация и выделение нарушений 2-го уровня путем выявления совокупности (двух-трех) отклонений 1-го уровня.

Отклонениями от штатных характеристик 3-го уровня считаются действия провокационного характера, 4-го и 5-го уровня – соответственно, опасные и явно враждебные ситуации или действия.

Нарушения 3-го, 4-го и 5-го уровней выводятся на пульт физической защиты и классифицируются как экстремальные ситуации, по которым оперативно должны приниматься меры. В отличие от них нарушения 1-го и 2-го уровня автоматически обрабатываются в базе данных и знаний и позволяют выделять потенциальных злоумышленников. Процесс видеорегистрации описывается выражением:

$$\frac{\partial j(\Lambda, t)}{\partial t} = -\frac{\partial}{\partial \Lambda} [K_1(\Lambda, t)j(\Lambda, t)] + \frac{\partial^2}{2\partial \Lambda^2} [K_2(\Lambda, t)j(\Lambda, t)] \quad (2)$$

Оно показывает возможность фиксирования контактов нарушителя или злоумышленника, опознанного по оперативной базе данных. Если процесс $\Lambda(t)$ ограничен, то есть $a < \Lambda < R$, где a – внешний периметр объекта, R – радиус его контролируемой зоны, то уравнение (2) следует рассматривать только внутри этой области. С физической точки зрения это означает, что если нарушитель или злоумышленник, чей образ имеется в оперативной базе данных, будет зарегистрирован (сфотографирован) видеосистемой, то он обязательно будет выявлен.

Процесс оптимального приведение состояния ситуационного фона лиц, находящихся в контролируемой зоне охраняемого объекта, из нештатного состояния в штатное

Моделируя работу систем наружного наблюдения, будем использовать белый шум и винеровский процесс. Белый шум не является марковским процессом, однако основное его свойство – независимость значений для любых сколь угодно малых промежутков между сечениями – не противоречит признаку марковости. Для марковского процесса и белого шума двумерная плотность вероятности выражается соотношением (3)

$$w_2(x_1, t_1, x_2, t_2) = w(x_1, t_1) w(x_2, t_2) \quad (3)$$

У белого шума в качестве плотности вероятности перехода выступает одномерное распределение в последующий (будущий) момент времени.

Поскольку контролируемая зона условно обозначается границей окружности радиуса R , а фактически имеет геометрическую конфигурацию, вводится дополнительный параметр d – расстояние до самой удаленной точки, контролируемой видеосистемами охраняемого объекта.

Если поток людей, проходящий через контролируемую зону, описывается белым шумом $n(t)$, а регистрация (фотосъемка) людей видеосистемами, находящимися в контролируемой зоне, представляет собой $\Lambda(t)$, то основные характеристики процесса регистрации лиц, находящихся в контролируемой зоне, будут определяться выражениями (4) – среднее значение и (5) – дисперсия:

$$m_\Lambda(t) = \Lambda_0 e^{-at} \quad (4)$$

$$s_\Lambda^2(t) = \frac{N_0 a}{4} (1 - e^{-2at}) \quad (5)$$

В начальный момент времени t_0 закономерность изменения плотности распределения вероятности определяется d -функцией, точнее $j_0(\Lambda, t_0) = d(\Lambda - \Lambda_0)$. С течением времени дисперсия растёт, и когда $m_\Lambda(t)$ достигает цели, дисперсия увеличивается до максимального значения, равного $\frac{N_0 a}{4}$. Процесс становится стационарным, и его плотность распределения уже не зависит от времени, то есть $j_{cm}(\Lambda, t) = j_{cm}(\Lambda)$. Значит, регистрация или выявление нарушителя или злоумышленника по образу, находящемуся в оперативной базе данных системы видеонаблюдения, не зависит от времени (продолжительности) присутствия его в контролируемой зоне.

Объединяя приведенные выше зависимости в систему уравнений, получим искомую математическую модель:

$$\left\{ \begin{array}{l}
 j(\Lambda) = \frac{1}{R}, \\
 j(\Lambda) = \left(1 - \frac{\Lambda_0}{R}\right) d(\Lambda) + \frac{\Lambda_0}{R} d(\Lambda - R), \\
 \frac{\partial j(\Lambda, t)}{\partial t} = -\frac{\partial}{\partial \Lambda} [K_1(\Lambda, t) j(\Lambda, t)] + \frac{\partial^2}{2\partial \Lambda^2} [K_2(\Lambda, t) j(\Lambda, t)], \\
 w_2(x_1, t_1, x_2, t_2) = w(x_1, t_1) w(x_2, t_2), \\
 m_\Lambda(t) = \Lambda_0 e^{-at}, \text{ где } a = \frac{1}{DR}, \\
 S_\Lambda^2(t) = \frac{N_0 a}{4} (1 - e^{-2at})
 \end{array} \right. \quad (6)$$

Вывод

Математическая модель выявления нестандартных ситуаций террористического характера с использованием фотографических образов людей, находящихся около объекта критической инфраструктуры, представляет собой систему шести уравнений. Первые два уравнения описывают хаотическое перемещение людей в контролируемой зоне вокруг объекта и показывают, что гости или командированные рано или поздно покинут пределы контролируемой зоны, а персонал охраняемого объекта и постоянно проживающие в зоне ограничивают свои перемещения внутри контролируемой зоны. Третье уравнение характеризует процесс видео регистрации нарушений 1-го и 2-го уровня, их систематизацию в базе данных и знаний и возможность выявления потенциальных злоумышленников по нетипичным элементам их поведения. Три последних уравнения описывают параметры процесса выявления злоумышленника по образу, находящемуся в оперативной базе данных системы видеонаблюдения.

Литература

1. Инфраструктура (Infrastructure) – это. Доступ: http://forexaw.com/TERMs/Industry/Plants_and_soobruzheniya/1853.pdf
2. Соловьев В.П. Инновационная инфраструктура как фактор социальной адаптации к условиям технологического развития. Доступ: <http://iee.org.ua/files/pub/svpinfr.pdf>
3. Инновационная инфраструктура 2017-2021. Доступ: https://www.eduget.com/news/innovacionnaya_infrastruktura_2017-2021-357
4. Рыночная инфраструктура. Доступ: <http://econominfo.ru/view-article.php?id=31>
5. Инфраструктура рынка. Доступ: <http://www.megos.org.ua/navczannia/ru/tema7.1.polit.page.html>
6. Информационная инфраструктура. Доступ: <https://ru.wikipedia.org/wiki/%D0%98%D0>
7. Военная инфраструктура. Доступ: http://safety_buildings.academic.ru/71/%D0%92%D0
8. Critical infrastructure – content, structure and problems of its protection. Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws
9. Хофрейтер Л. Критическая инфраструктура – содержание, структура и проблемы ее защиты. Доступ: <http://jml2012.indexcopernicus.com/fulltxt.php?ICID=1129729>
10. Указ Президента України №8/2017 від 16 січня 2017 року. Доступ: <http://www.president.gov.ua/documents/82017-21058>
11. Порошенко усилил защиту объектов критической инфраструктуры. Доступ: http://news.liga.net/news/politics/14672613poroshenko_usilil_zashchitu_obektov_kriticheskoy_infrastruktury.htm
12. Гончаренко Ю.Ю. Оценка эффективности управления чрезвычайной ситуацией / Ю.Ю. Гончаренко, Е.В. Азаренко, Ю.В. Браславский и др. // Сб. науч. тр. СНУЯЭиП. – Вып. 2 (38). – Севастополь: СНУЯЭиП, 2011. – С. 239 – 245.

References

1. Infrastruktura (Infrastructure) – eto. Dostup: http://forexaw.com/TERMs/Industry/Plants_and_soobruzheniya/1853.pdf
2. Solovyev V. P. Innovatsionnaya infrastruktura kak faktor sotsialnoyi adaptatsii k usloviyam tehnologicheskogo razvitiya. Dostup: <http://iee.org.ua/files/pub/svpinfr.pdf>
3. Innovatsionnaya infrastruktura 2017-2021. Dostup: https://www.eduget.com/news/innovacionnaya_infrastruktura_2017-2021-357
4. Ryinochnaya infrastruktura. Dostup: <http://econominfo.ru/view-article.php?id=31>
5. Infrastruktura ryinka. Dostup: <http://www.megos.org.ua/navczannia/ru/tema7.1.polit.page.html>
6. Informatsionnaya infrastruktura. Dostup: <https://ru.wikipedia.org/wiki/%D0%98%D0>
7. Voennaya infrastruktura. Dostup: http://safety_buildings.academic.ru/71/%D0%92%D0
8. Critical infrastructure – content, structure and problems of its protection. Input: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE&gws
9. Hofreyiter L. Kriticheskaya infrastruktura – sodershanie, struktura i problemti ee zashityi. Dostup: <http://jml2012.indexcopernicus.com/fulltxt.php?ICID=1129729>
10. Ukaz Prezidenta Ukrainyi №8/2017 bid 16 schnya 2017 roku. Dostup: <http://www.president.gov.ua/documents/82017-21058>
11. Poroshenko usilil zashitu ob'ektov kriticheskoy infrastrukturu. Dostup: http://news.liga.net/news/politics/14672613poroshenko_usilil_zashchitu_obektov_kriticheskoy_infrastruktury.htm
12. Goncharenko Yu. Yu. Otsenka effektivnosti upravleniya chrezvyichaynoy situatsiyey / Yu. Yu. Goncharenko, E. V. Azarenko, Yu. Yu. Braslavskiy i dr. // Sb. nauch. tr. SNUYAiP. – Vyip. 2 (38). – Sevastopol: SNUYAiP, 2011. – S. 239 – 245.

Отримана/Received : 25.9.2017 р. Надрукована/Printed : 9.10.2017 р.
Стаття рецензована редакційною колегією