Виктор В. Ерохин[1], Лариса С. Притчина[2]
[1,2]Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации,
пр-т Вернадского, 76, Москва, 119454, Россия
[1]e-mail: erohinvv@mail.ru, https://orcid.org/0000-0002-8754-0012
[2]e-mail: larisa.pritchin@gmail.com, https://orcid.org/0000-0001-6566-8894

МОДЕЛИРОВАНИЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ОХРАНЯЕМОГО ОБЪЕКТА НА ОСНОВЕ ТЕОРИИ АВТОМАТОВ И СЕТЕЙ ПЕТРИ

DOI: http://dx.doi.org/10.26583/bit.2020.1.05

Аннотация. В статье рассматриваются задачи по оценке и моделированию действий подразделений ОВД или других охранных структур по организационной защите охраняемого объекта на основе теории автоматов и сетей Петри. Решением задачи по созданию модели действий злоумышленника на охраняемом объекте на базе теории автоматов является определение времени пребывания злоумышленника на охраняемом объекте. Решением задачи по моделированию организационной защиты охраняемого объекта с использованием сетей Петри является нахождение параллельно реализующихся взаимосвязанных процессов действия охранных подразделений при осуществлении специальных операций. Рассмотрены методы решения защищаемого объекта от действий злоумышленника: модель организационной защиты охраняемого объекта от действий злоумышленника на основе теории автоматов; модель организационной защиты на основе сетей Петри. Проведено моделирование системы защиты объекта во времени с учётом особенностей угроз, как от субъектов уголовного мира, так и при чрезвычайных ситуациях. Представленные подходы и методы моделирования действий охранных структур позволяют оценить их действия.

Ключевые слова: защита информации, сети Петри, теория автоматов.
Для цитирования: ЕРОХИН, Виктор В.; ПРИТЧИНА, Лариса С. МОДЕЛИРОВАНИЕ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ОХРАНЯЕМОГО ОБЪЕКТА НА ОСНОВЕ ТЕОРИИ АВТОМАТОВ И СЕТЕЙ ПЕТРИ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 65-77, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1271>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.05.

Viktor V. Erokhin[1], Larisa S. Pritchina[2]
[1,2]Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs,
76 Vernadsky Ave., Moscow, 119454, Russia
[1]e-mail: erohinvv@mail.r, https://orcid.org/0000-0002-8754-0012
[2]e-mail: larisa.pritchin@gmail.com, https://orcid.org/0000-0001-6566-8894

Simulation of organizational protection of a protected object based on the theory of automata and Petri nets

DOI: http://dx.doi.org/10.26583/bit.2020.1.05

Abstract. The paper discusses the tasks of evaluating and modeling the actions of police units or other security structures for the organizational protection of a guarded object based on the theory of automata and Petri nets. The solution to the problem of creating a model of an attacker's actions on a guarded object on the basis of the theory of automata is to determine the time of an attacker's stay on a guarded object. The solution to the problem of modeling the organizational protection of a protected facility using Petri nets is to find parallel-to-work interconnected processes of security units during special operations. The methods of solving the protected object from the actions of an attacker are considered: a model of organizational protection of the protected object from the actions of an attacker based on the theory of automata; model of organizational protection based on Petri nets. This allows simulating the object's

protection system in time taking into account the specifics of threats both from the subjects of the criminal world and in emergency situations. In addition the presented approaches and modeling methods for the actions of security structures allow the most accurate assessment and optimization of their actions.
Keywords: information protection, Petri nets, automata theory.
For citation: EROKHIN, Viktor V.; PRITCHINA, Larisa S. Simulation of organizational protection of a protected object based on the theory of automata and Petri nets. IT Security (Russia), [S.l.], v. 27, n. 2, p. 65-77, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1271>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.05.

Введение

Деятельность злоумышленников оказывают достаточное сильное влияние на ущемление прав и свобод человека, на его стремление к комфортной жизни и на функционирование организационных систем в целом. Для эффективной борьбы с деятельностью злоумышленников необходимо принять упреждающие его деятельность специальные меры по организационной защите охраняемого объекта и его субъектов и объектов функционирования.

Последствиями действий злоумышленника обычно являются возникновение угроз жизнеобеспечению человека, его правам и свободам, нанесению материально-финансового ущерба организационной системе или отдельному человеку, по нарушению условий жизни населения и работы правительственных органов и т.д.

Основной объём специальных мероприятий по борьбе с угрозами охраняемых объектов проводится подразделениями УВД. Например, такими мерами могут быть:

- пресечение деятельности уголовных элементов и незаконных вооруженных формирований;
- розыск и задержание злоумышленников и преступников;
- охрана объектов и субъектов;
- сдерживание восстаний и массовых беспорядков;
- освобождение заложников;
- ликвидация последствий чрезвычайных ситуаций.

1. Постановка задачи исследования

Для результативного предупреждения и устранения угроз, а также последствий чрезвычайных ситуаций, необходимо создать математические модели действий охранных подразделений и его персонала при возникновении чрезвычайных обстоятельств. Характер таких действий имеет зависимость от особенностей развития угроз объекту защиты (от злоумышленников, чрезвычайных ситуаций). В связи с чем появляется задача – необходимость в оценивании результативности и оптимизации действий охранных подразделений с учётом различных видов угроз и имеющихся людских и технических ресурсов.

Угрозы охраняемому объекту могут иметь следующие особенности:

- уникальны в совокупности по характеру, физической и социальной среде реализации;
- быстрота развития и реализации;
- как правило, нечеткая определенность исходных данных;
- неполнота и нецелостность исходных данных;
- поэтапное развитие и реализация;
- стохастичность действий.

На основе анализа указанных особенностей развития и реализации угроз на охраняемом объекте, можно определиться с математическим аппаратом по моделированию действий охранных подразделений и их структур. Так как развитие чрезвычайной ситуации на охраняемом объекте происходит поэтапно, то это обусловливает осуществление дискретизации описания такой ситуации посредством методов теории конечных автоматов, сетей Петри, графов. Если в организационной системе охраны объекта присутствует стохастичная сменность состояний, тогда дополнительно к указанным методам необходимо применить модели Марковских и полумарковских цепей и вероятностных автоматов [1–4].

На выбор математических методов моделирования организационной системы по охране объекта могут оказывать следующие характеристики:

- количество охранных структур и групп, которые принимают участие в устранении чрезвычайных ситуаций;
- допустимость риска;
- точность экстраполяции развития чрезвычайных ситуаций на охраняемом объекте;
- сложный или простой характер развития чрезвычайных ситуаций.

На основе этих характеристик можно применять при охране объекта различные виды математического моделирования действий охранных структур по охране объекта и поимке нарушителей (злоумышленников). Присутствие большого количества охранных структур обусловливает при моделировании организационных систем охраны объекта использовать методы теории автоматов. Для чрезвычайных ситуаций с небольшим количеством охранных структур для математического моделирования их действий оптимально использовать Марковские модели или методы теории сетей Петри. Если в организационной системе охраны объекта основной характеристикой является допустимость риска, тогда для моделирования действий охранных структур уже оптимально использовать методы теорий конфликта и игр [5]. В системе охраны объекта, где необходимо обеспечить точность экстраполяции развития чрезвычайных ситуаций на охраняемом объекте, наиболее оптимально для моделирования действий охранных структур использовать методы теории сетей Петри (обеспечение точного результата), Марковские модели (приближенная экстраполяция). При сложном характере развития чрезвычайных ситуаций на объекте охраны оптимальным является применении комбинации методов: сетей Петри, теории автоматов, Марковских моделей, нечетких множеств, теории игр и т.д.

Существуют большие возможности в выборе моделей, которые учитывают динамику изменений состояний моделируемой организационной системы. Особенно эффективными являются модели на основе [1, 4, 6]:

- теории автоматов, которые позволяют оценить разнообразные показатели функционирования моделируемой организационной системы в виде охраняемого объекта;
- сетей Петри.

Использование теории автоматов основано на характеристиках преобразователей – дискретность функционирования и конечность описываемых ими диапазонов параметров [1, 7]. Еще одна важная особенность дискретных моделей заключается в том, что они не используют количественные, а только качественные характеристики для определения текущего состояния модели. Изменения в состоянии дискретной модели от момента к моменту могут быть либо детерминированными, либо недетерминированными.

Первоначально рассмотрим задачу разработки модели действий злоумышленника на охраняемом объекте на основе теории автоматов. Решением задачи является определение времени пребывания злоумышленника на охраняемом объекте.

Далее рассмотрим задачу определения параллельно реализующихся взаимосвязанных процессов действия охранных подразделений при осуществлении специальных операций по организационной защите охраняемого объекта с использованием моделирования на основе сетей Петри.

2. Методы решения защищаемого объекта от действий злоумышленника

2.1. Модель организационной защиты охраняемого объекта от действий злоумышленника на основе теории автоматов.

Повышенный уровень организационной защиты охраняемых объектов от криминального вмешательства обеспечивается применением необходимых технических средств в сочетании с высококачественным оборудованием систем безопасности и сигнализации. Охраняемые объекты в зависимости от важности, количества и типа значений делятся на две категории и четыре подкатегории. Для всех подкатегорий охраняемых объектов имеются разнообразные способы их организационной защиты, что предполагает использование нескольких линий защиты. При анализе охраняемого объекта, как правило, рассматриваются три типа линии защиты:

1) осуществление контроля периметра охраняемого объекта или его элементов;
2) проведение контроля помещений;
3) контролирование хранилищ ценных объектов.

Несколько рубежей указанных типов может присутствовать на охраняемом объекте [1]. При этом злоумышленники преодолевают линии защиты последовательно, и на каждой из линий защиты совершаются или не совершаются какие-либо события, которые являются следствием действий злоумышленников или организационной системы охраняемого объекта. В частности [8, 9]:

- система охраны может либо обнаружить или не обнаружить преступника (злоумышленника);
- в зависимости от вида организационной системы охраняемого объекта злоумышленник при его выявлении может быть информирован или не информирован;
- после обнаружения злоумышленника сигнал от системы защиты объекта поступает на центральную станцию безопасности. Группа задержания или охрана выдвигается к охраняемому объекту для пресечения правонарушения либо для поимки злоумышленника.

При этом на центральную станцию безопасности может поступить ложный сигнал тревоги, который в большинстве случаев обусловливается внешними какими-либо воздействиями или явлениями искусственного/естественного происхождения.

Для математического моделирования организационной защиты охраняемого объекта требуется задать её параметры (g, s, v, $\underline{z}$), такие как:

- если нарушитель преодолел j-ю (j = 1, 2, 3) линию защиты, тогда $g_j = 1$;
- если нарушитель отступил через j-ю линию защиты, тогда $\overline{g}_j = 1$;
- если нарушитель не обнаружен на j-й линии защиты, тогда $s_j = 1$;
- если нарушителя не обнаружили при отступлении через j-ю линию защиты, тогда $\overline{s}_j = 1$;
- если нарушителя не задержали, тогда $v_1 = 1$;
- если были похищены или повреждены ценности, тогда $v_2 = 1$;
- если на j-й линии защиты сработал ложный сигнал тревоги, тогда $z_j = 1$.

- во всех иных случаях параметры g, s, v, z равняются нулю.

С использованием назначенных параметров логики g, s, v, z возможно смоделировать любые действия нарушителя, а также на эти действия реакцию организационной системы защиты охраняемого объекта:

- если нарушитель преодолел первую линию защиты и система охраняемого объекта его обнаружила, тогда $g_1 \,\&\, \bar{s}_1 = 1$;
- если нарушитель перешёл первую и вторую линию защиты, но не смог преодолеть третью линии защиты, и отступил через вторую линию защиты, был выявлен при преодолении второй линии защиты, тогда $g_1 \,\&\, s_1 \,\&\, g_2 \,\&\, \bar{s}_2 \,\&\, \bar{g}_2 \,\&\, \bar{s}_2 = 1$.

Далее приведены результаты математическое моделирование действий нарушителя на объекте охраны на основе конечного аппарата Мура:

$M = (P, X, Y, \delta, \chi)$,

где M – конечный аппарат Мура, описываемый пятиместным кортежем; P – алфавит действий нарушителя на объекте охраны и реакция организационной системы защиты охраняемого объекта; X – входной алфавит воздействий, обусловливающих смену действий нарушителя; Y – выходной алфавит оценивания времени пребывания нарушителя в каждом своем действии на объекте охраны; $\delta: P \times X \to P$ – функция переходов; $\chi: P \to Y$ – функция выходов [1, 10–12].

Автоматная модель охраняемого объекта описывает переходы в промежуточное состояние по параметру P_{ji}, где j – номер преодолеваемой линии защиты, которую преодолел нарушитель, если нарушитель не преодолел линию защиты или отступает через соответствующую линию защиты, тогда перед j ставиться знак минус; i – тип реакции организационной системы охраны объекта: $i = 1$ – нарушитель линии защиты не выявлен; $i = 2$ – нарушитель линии защиты выявлен; $i = 3$ – сработала ложная сигнализация; $i = 4$ – нарушитель смог скрыться с охраняемого объекта; $i = 5$ – информация о задержании нарушителя.

Например, смена действия нарушителя фиксируется компонентами входного алфавита, который определяется следующими логическими выражениями:

- модель $X_{0,12} = \langle g_1 \,\&\, \bar{P}_1 = 1 \rangle$ определяет переход действия нарушителя P_0 в P_{12};
- модель $X_{22,42} = \langle \bar{g}_2 \,\&\, \bar{s}_2 = 1 \rangle$ определяет переход действия нарушителя P_{22} в P_{42}.

В автоматной модели Мура выходные элементы (Y_j) определяются только действиями нарушителя.

При перемещении нарушителя по охраняемому объекту происходит смена его действий от первоначального P_0 (состояние «нормы») до одного из конечных действий, например:

- если нарушителем были похищены ценности, и он смог скрыться, тогда $P_4 = 1$;
- если нарушителем не были похищены ценности, и он смог скрыться, тогда $P_4 = 0$;
- если нарушителя задержали, тогда $P_5 = 1$;
- если нарушителя не задержали, тогда $P_5 = 0$.

Автоматная модель описывает потенциальные вариации для нарушителя, проходящего охрану объекта, как с техническими средствами защиты, так и без них, с учетом времени, затрачиваемого для преодоления каждой линии защиты. Поскольку существует несколько способов организации защиты объектов, необходимо осуществить синтез моделей Мура. Синтез модели конечного автомата выполняется за счет определения последовательности изменений действий нарушителя в зависимости от его точки проникновения, потенциального поведения, использования технических средств защиты, сигнализации, вероятности поимки нарушителя и т.д. На рис. 1 представлен

пример последовательности изменений в автоматной модели, которая имитирует действия нарушителя, который преодолевает последовательно все линии защиты охраняемого объекта. При этом нарушитель был выявлен при пересечении второй линии защиты и захвачен охраной объекта после пересечения им третьей линии защиты.

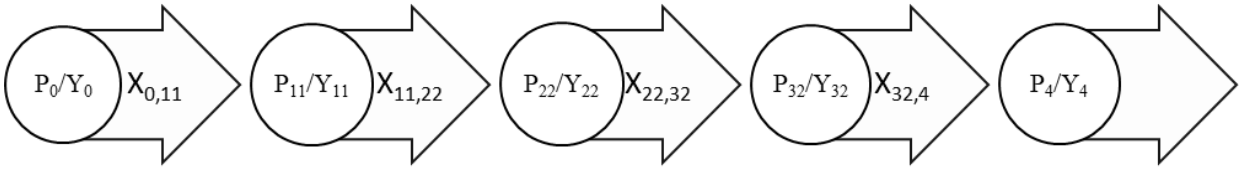


Рис. 1. Последовательность действий в автоматной модели системы защиты
(Fig. 1. Sequence of actions in the automatic security system model)

Для большей детализации организационной системы защиты охраняемого объекта необходимо применить дополнительные логические параметры. Однако это повысит размерность автоматной модели, что скажется на времени реагирования системы на действия нарушителя.

Для оценивания времени преодоления нарушителем организационной системы защиты охраняемого объекта зададим следующие параметры: t_j – время пребывания организационной системы защиты объекта охраны в состоянии P_j (стохастический параметр). На параметр t_j по преодолению нарушителем каждой из линии защиты влияет совокупность стохастических факторов, таких как тип и качественные характеристики инженерно-технической защиты охраняемого объекта, вероятность выявления нарушителя, вид объекта защиты и его площадь или объем и др. Применяя теорему Ляпунова и из источников [1, 7, 10, 13], можно задать, что Y_j имеет нормальный закон распределения с математическим ожиданием m_j и дисперсией d_j.

Посредством предложенной модели организационной защиты охраняемого объекта на основе теории автоматов можно определить время нахождения злоумышленника на охраняемом объекте.

Предложенные аспекты по построению автоматной модели организационной защиты охраняемого объекта позволяют:

- анализировать длительности пребывания нарушителя на объекте охраны с учетом его времени преодоления каждой линии защиты;
- преобразовать автоматную модель в имитационную посредством определения вероятностных значений параметров g_j, s_j, v_j, z_j.

Построим динамическую модель действий охранных структур для ликвидации чрезвычайных ситуаций на охраняемом объекте (рис. 2). При развитии чрезвычайной ситуации охранные структуры реализуют следующие действия: P_0 – повседневная деятельность охранных структур; P_1 – сбор, группировка, классификация и анализ данных о потенциальной чрезвычайной ситуации, их уточнение и предварительное оценивание ситуации; P_2 – предварительные директивы или приказы охранным структурам; P_3 – формирование решений, определение тактических действий охранным структурам, выбор управляющих действий, организация сил и средств для ликвидации чрезвычайных ситуаций, постановка задач охранным структурам; P_4 – управление охранными структурами, определение порядка взаимодействия с другими силами; P_5 – осуществление решения поставленной задачи охранными структурами; P_6 – охранные структуры

завершают действия по охране объекта; P_7 – подведение итогов в работе охранных структур.

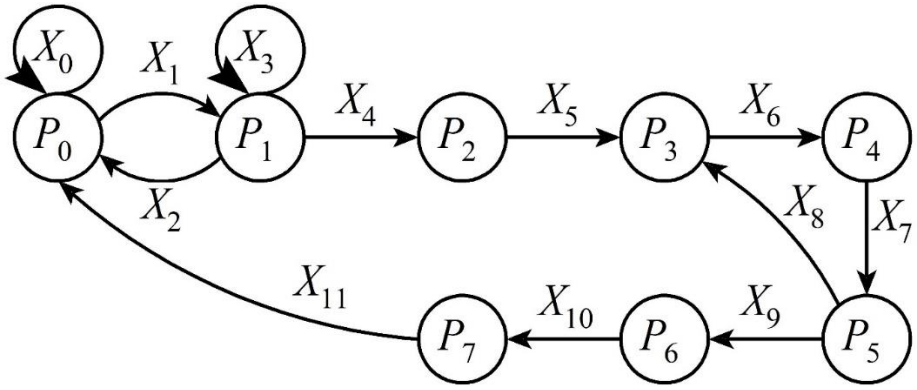
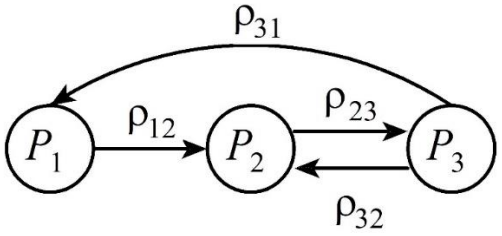


Рис. 2. Автоматная модель действий охранных структур при ликвидации чрезвычайной ситуации на охраняемом объекте
(Fig. 2. Automatic model of actions of security structures in the event of an emergency at a protected object)

Представим моделирование действий охранных структур при проведении мероприятия по поиску и аресту вооруженных нарушителей (рис. 3): P_1 – охранная структура выдвигается на охраняемый объект; P_2 – охранной группой был перекрыт подступ в зону охраняемого объекта, P_3 – охранная структура выдвигается на опорный пункт. На рис. 3 представлен граф рассматриваемой организационной системы охраны с тремя состояниями (P_1, P_2, P_3) и его матричное отображение. Состояния и действия охранных структур известны. Смена этих состояний осуществляется достаточно быстро, чтобы считать такую смену дискретной, и в заданное время.



$$\left[\rho_{ij}\right]=\begin{Vmatrix} 0 & \rho_{12} & 0 \\ 0 & 0 & \rho_{23} \\ \rho_{31} & \rho_{32} & 0 \end{Vmatrix}$$

Рис. 3. Граф состояний и переходов действий охранных структур при проведении мероприятия по поиску и аресту вооруженных нарушителей и его матричное отображение
(Fig. 3. Graph of States and transitions of actions of security structures during the search and arrest of armed violators and its matrix representation)

Для каждого перехода из одного состояния в другое пусть будут заданы вероятности ρ_{ij} системы состояний P. Задачей данного моделирования является расчет вероятностей $\rho_j(k)$ нахождения организационной системы охраны объекта после k-го шага в каждом j-м состоянии. В форме ориентированного графа состояний и переходов представляется организационная система охраны объекта. Вершинами графа являются состояния организационной системы. Дуги графа определяют направления потенциального перехода системы из какого-либо состояния в другое. Дуги на графе не изображаются в случаях, если вероятность перехода организационной системы из одного состояния в другое равняется нулю. Например, для рассматриваемой системы

нейтрализации вооруженных нарушителей вероятность перехода ρ_{12} из состояния P_1 в состояние P_2 будет зависеть от качества постановки задач охранной структуре. Вероятность перехода ρ_{23} из состояния P_2 в состояние P_3 будет зависеть от распоряжения о выдвижении сотрудников охранной структуры на опорный пункт. Вероятность перехода ρ_{31} из состояния P_3 в состояние P_1 будет зависеть от распоряжения о выдвижении сотрудников охранной структуры на охраняемый объект.

2.2. Моделирование организационной защиты на основе сетей Петри

Быстрота формирования чрезвычайных ситуаций на охраняемом объекте при лимитированном времени на исполнение охранных задач или мероприятий, а также неполные исходные данные обусловливают невозможность принятия результативных решений по управлению организационной защитой объекта охраны. Для таких систем рационально использовать методы адаптивного управления организационными системами [1, 14, 15]. В большинстве случаев действия охранных структур на охраняемом объекте при появлении чрезвычайных ситуаций являются кибернетическими, где осуществляется действие управляющего органа на управляемый объект охраны для обеспечения требуемого уровня охраны или перевода процессов в охраняемом объекте в желаемые.

Для моделирования параллельно действующих взаимосвязанных процессов в больших организационных системах (например, действия охранных структур при осуществлении специальных операций при устранении чрезвычайных ситуаций) наиболее широко применяются сети Петри. Сети Петри позволяют учитывать структурность организационной системы охраны объекта и действующие в ней процессы, а также её функционал.

Рассмотрим устоявшуюся организационную систему охраняемого объекта в виде трёх её компонентов (рис. 4): оперативный штаб; охранные структуры или группы (ОГ); чрезвычайные ситуации на охраняемом объекте. В организационной системе охраны объекта управляемыми объектами являются единицы совокупности чрезвычайных ситуаций [4, 12].

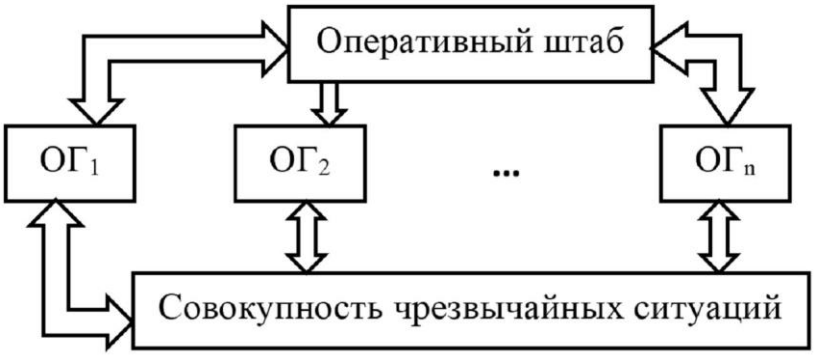


Рис. 4. Модель организационной системы охраняемого объекта
(Fig. 4. Model of the organizational system of the protected object)

Для ликвидации чрезвычайных ситуаций, как проникновение нарушителя или иное, должны использоваться управляющие воздействия – проведение специальных мероприятий и действий охранными структурами. Путем изменений состояний управляемого объекта охраны обеспечивается модификация действий в организационной системе защиты объекта, т.е., например, видоизменение тактических действий охранных подразделений.

Прогнозным или экспертным оцениванием можно компенсировать частичную стохастичность и неполноту исходных данных. Для получения исходных данных, как правило, применяют методы теории вероятности и математической статистики, теории нечетких множеств. Например, при проникновении на охраняемом объекте неизвестного количества нарушителей, их вооружение, интересы и т.д., для описания такой чрезвычайной ситуации на охраняемом объекте необходимо воспользоваться методами теории нечетких множеств. Анализируя данные криминогенных ситуаций по охраняемым объектам, можно утверждать, что количество нарушителей не менее 2 человек и не более 11, но вероятнее всего 4 или 5 человек (рис. 5).

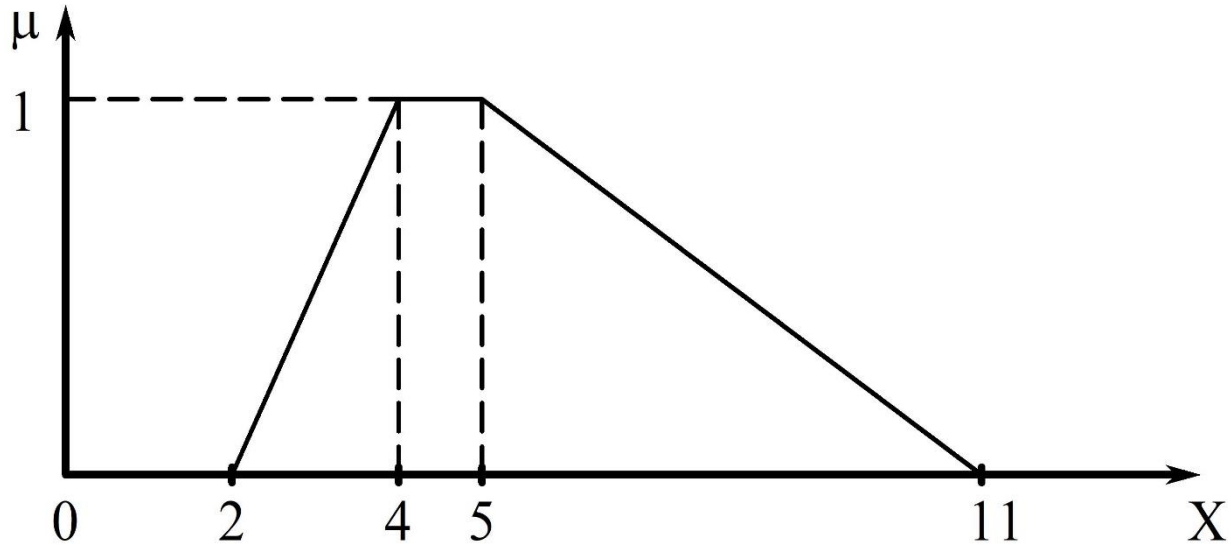


Рис. 5. Трапециевидный закон распределения нарушителей на охраняемом объекте)
(Fig. 5. Trapezoidal law of distribution of the number of violators of the protected object)

Аналитическая форма задания функции $\mu(X)$ следующая:

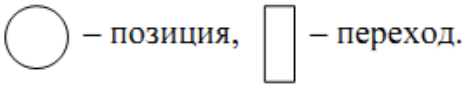
$$\mu = \begin{cases} 0, if \;\; x \le 2 \; or \; x \ge 11, \\ 0{,}5x - 1, if \;\; 2 \le x < 4, \\ 1, if \;\; 4 \le x < 5, \\ -\frac{1}{6}x + 1\frac{5}{6}, if \;\; 5 \le x < 11. \end{cases}$$

Если система охраны объекта располагает совокупностью даже приблизительных параметров чрезвычайных ситуаций, тогда появляется возможность рассчитать функции принадлежности $\mu(x)$.

Сети Петри описывают системы, которые состоят из набора взаимодействующих подсистем. Подсистемы работают в последовательном и параллельном режимах. Принимается во внимание, что каждая подсистема состоит из подсистем нижнего уровня – иерархическая структура. Сети Петри позволяют описать независимое поведения подсистем. Однако при этом необходима объективная информация о взаимодействии между подсистемами одного и того же уровня. С использованием сетей Петри можно не только осуществлять имитирование функционирования систем, но и представлять

информационные процессы, такие как управление организационной системой охраны объекта [10].

В графическом отображении сети Петри зададим два вида узла:



В любой момент времени каждая охранная группа может находиться в некотором состоянии. В соответствии с распоряжениями, приказами, директивами вышестоящей структуры охраны объекта осуществляется переход из одного состояния в другое. После перехода в следующее состояние руководитель охранной группы рапортует об исполнении (неисполнении) поставленной перед группой задачи.

Модель действий охранной группы (ОГ) при осуществлении мероприятий по поимке нарушителя на объекте охраны приведена на рис. 6.

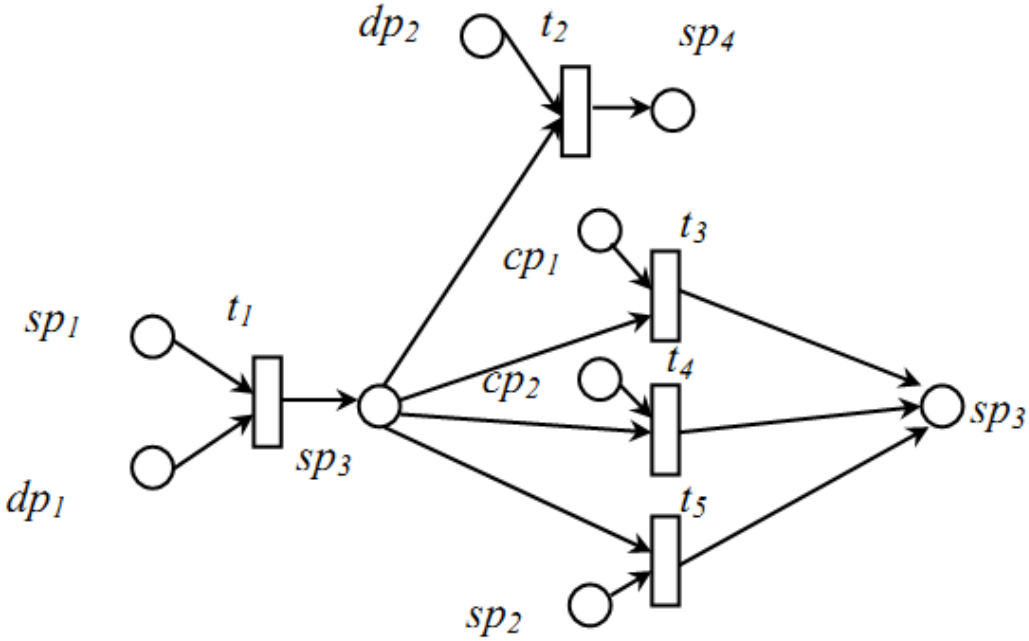


Рис. 6. Модель действий охранной группы
(Fig. 6. Security group action model)

На рис. 6 представлены следующие позиции и переходы данной модели:
*sp*1 – создана охранная группа;
*sp*2 – объект охраны покидает обслуживающий персонал;
*sp*3 – охранная группа осуществляет контроль доступа на объект охраны;
*sp*4 – расформирована или переформирована охранная группа;
*cp*1 – на охранный объект происходят попытки проникновения нарушителей;
*cp*2 – охраняемый объект пытаются покинуть нарушители;
*dp*1 – перед охранной группой поставлены задачи по охране объекта;
*dp*2 – приказ о расформировании или переформировании охранной группы;
*t*1 – охраняемая группа заняла позиции;
*t*2 – расформирование или переформирование охранной группы;

*t*3 – охранная группа препятствует продвижению нарушителей на охраняемый объект или пересечение ими линий защиты;

*t*4 – охраняемой группой пойманы и нейтрализованы нарушители;

*t*5 – охраняемая группа возвращает украденные ценности с охраняемого объекта.

Если при ликвидации чрезвычайных ситуаций на охраняемом объекте привлекаются в большом количестве различные по своему функциональному назначению охранные группы, тогда применение моделирования на основе сетей Петри дает менее точный результат из-за громоздкости. В этом случае целесообразно применять моделирование на основе теории автоматов.

Заключение

Предложенная автоматная модель имеет следующие преимущества: мониторинг продолжительности пребывания нарушителей на охраняемом объекте по каждому рубежу; модель может использовать стохастические значения алфавита действий нарушителя на объекте охраны и реакции организационной системы защиты охраняемого объекта, что позволит рассмотреть эту модель, как имитационную, которая позволит решать оптимизационные задачи.

Представленные подходы и методы моделирования действий охранных структур на охраняемом объекте учитывают характеристики выполняемых задач в случаях появления чрезвычайных ситуаций, что позволяет оценить действия охранных структур.

СПИСОК ЛИТЕРАТУРЫ:

1. Абрамов П.Б. Моделирование динамики сложных систем на основе Марковских форм с внешними потоками событий / П.Б. Абрамов. – Воронеж: ВУНЦ ВВС ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина, 2013. – 156 с.
2. Motallebi H., Abdollahi Azgomi M. Translation from Multisingular Hybrid Petri Nets to Multisingular Hybrid Automata // Fundamenta Informaticae, Vol. 130, No. 3, IOS Press, Feb. 2014. P. 275–315. DOI: 10.3233/FI-2014-993.
3. Chang L., He X., Shatz S. M. A methodology for modeling multi-agent systems using nested petri nets // International Journal of Software Engineering and Knowledge Engineering, Vol. 22, No. 2012. P. 891–925. DOI: 10.1142/S0218194012500246.
4. Pla A., Gay P., Melendez J., Lopez B. Petri net-based process monitoring: A workflow management system for process modelling and monitoring // Journal of Intelligent Manufacturing, Vol. 25, No. 3, 2014. P. 539–554. DOI: 10.1007/s10845-012-0704-z.
5. Orojloo H., Abdollahi Azgomi M. A game-theoretic approach to model and quantify the security of cyber-physical systems // Computers in Industry, Vol. 88, Elsevier, 2017. P. 44–57. DOI: 10.1016/j.compind.2017.03.007.
6. Соломатин М.С., Рогозин Е.А., Дровникова И.Г. Создание модели информационного конфликта "Нарушитель - система защиты" на основе сети Петри-Маркова // Вестник Воронежского института МВД России. 2019. № 2. С. 93–100. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik2_2019.pdf (дата обращения: 20.02.2020).
7. Jan N.M., Fong W.H., Sarmin N.H. State machine of place-labelled petri net controlled grammars // Malaysian Journal of Fundamental and Applied Sciences 13(4), 2017. P. 649–653.
8. Занина Т.М. Некоторые аспекты административно-правового регулирования защиты информации на режимных объектах // Вестник воронежского института МВД России, 2018, 3. С. 124–127. URL: https://ви.мвд.рф/upload/site132/document_journal/vestnik_2018_3(2).pdf (дата обращения: 20.02.2020).
9. Козьминых С.И. Организация защиты информации в российской полиции / С.И. Козьминых. – М.: «Издательство «Юнити-Дана», 2017. – 407 с.
10. Zaitsev D.A., Shmeleva T.R., Retschitzegger W., Pröll B. Security of grid structures under disguised traffic attacks // Cluster Computing, 19(3) 2016, 1183–1200. Online 17 June 2016. DOI: 10.1007/s10586-016-0582-9. URL: https://link.springer.com/article/10.1007/s10586-016-0582-9 (дата обращения: 20.02.2020).
11. Мурзаханова Е.В., Пищухин А.М. Оптимальное распределение ресурсов в системе защиты информации в организации // Вопросы защиты информации. 2019. 2(125). С. 36–40.

URL:http://izdat.ntckompas.ru/editions/for_readers/archive/article_detail.php?SECTION_ID=155&ELEMENT_ID=24535 (дата обращения: 20.02.2020).

12. Солодянников А.В. Организация и управление службой защиты информации / А.В. Солодянников. – СПб.: Санкт-Петербургский государственный экономический университет, 2018. – 89 с. URL: https://elibrary.ru/item.asp?id=37310180 (дата обращения: 20.02.2020).
13. Мустафаев В.А., Салманова М.Н. Моделирование динамических взаимодействующих процессов с применением нечетких сетей Петри типа V_F // Вестник Воронежского государственного технического университета. 2019. Т. 15. № 3. С. 28–33. DOI: 10.25987/VSTU.2019.15.3.004. URL: https://cchgeu.ru/science/nauchnye-izdaniya/vestnik-voronezhskogo-gosudarstvennogo-tekhnicheskogo-universiteta-/fayly/vypuski/15_3.pdf (дата обращения: 20.02.2020).
14. Zaitsev D.A., Shmeleva T.R., Groote J.F. Verification of Hypertorus Communication Grids by Infinite Petri Nets and Process Algebra // IEEE/CAA Journal of Automatica Sinica, 6(3), 2019, 733–742. DOI: 10.1109/JAS.2019.1911486. URL: https://ieeexplore.ieee.org/document/8707130 (дата обращения: 20.02.2020).
15. Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. 4(17). С. 61–71. URL: https://elibrary.ru/item.asp?id=27441076 (дата обращения: 20.02.2020).

REFERENCES:

[1] Abramov P.B. Modelirovanie dinamiki slozhnyh sistem na osnove Markovskih form s vneshnimi potokami sobytij. P.B. Abramov. – Voronezh: VUNC VVS VVA im. prof. N.E. Zhukovskogo i Ju.A. Gagarina, 2013. – 156 s. (in Russian).
[2] Motallebi H., Abdollahi Azgomi M. Translation from Multisingular Hybrid Petri Nets to Multisingular Hybrid Automata. Fundamenta Informaticae, Vol. 130, No. 3, IOS Press, Feb. 2014. P. 275–315. DOI: 10.3233/FI-2014-993.
[3] Chang L., He X., Shatz S.M. A methodology for modeling multi-agent systems using nested petri nets. International Journal of Software Engineering and Knowledge Engineering, Vol. 22, No. 2012. P. 891–925. DOI: 10.1142/S0218194012500246.
[4] Pla A., Gay P., Melendez J., Lopez B. Petri net-based process monitoring: A workflow management system for process modelling and monitoring. Journal of Intelligent Manufacturing, Vol. 25, No. 3, 2014. P. 539–554. DOI: 10.1007/s10845-012-0704-z.
[5] Orojloo H., Abdollahi Azgomi M. A game-theoretic approach to model and quantify the security of cyber-physical systems. Computers in Industry, Vol. 88, Elsevier, 2017. P. 44–57. DOI: 10.1016/j.compind.2017.03.007.
[6] Solomatin M.S., Rogozin E.A., Drovnikova I.G. The creation of a model of the information conflict "Intruder - protection system" on the basis of Petri-Markov network. The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia. 2019. № 2. P. 93–100. URL: https://ви.мвд.рф/upload/site132/document_journal/Vestnik2_2019.pdf (accessed: 20.02.2020) (in Russian).
[7] Jan N.M., Fong W.H., Sarmin N.H. State machine of place-labelled petri net controlled grammars. Malaysian Journal of Fundamental and Applied Sciences 13(4), 2017. P. 649–653.
[8] Zanina T.M. Some aspects of administrative legal regulation of information security on regime objects. The bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia, 2018, 3. P. 124–127. URL: https://ви.мвд.рф/upload/site132/document_journal/vestnik_2018_3(2).pdf (accessed: 20.02.2020) (in Russian).
[9] Koz'minyh S.I. Organizacija zashhity informacii v rossijskoj policii / S.I. Koz'minyh. – M.: «Izdatel'stvo «Juniti-Dana», 2017. – 407 s. (in Russian).
[10] Zaitsev D.A., Shmeleva T.R., Retschitzegger W., Pröll B. Security of grid structures under disguised traffic attacks. Cluster Computing, 19(3) 2016, 1183–1200. Online 17 June 2016. DOI: 10.1007/s10586-016-0582-9. URL: https://link.springer.com/article/10.1007/s10586-016-0582-9 (accessed: 20.02.2020).
[11] Murzakhanova E.V., Pishchukhin A.M. Optimal allocation of resources in the information security system of the organization. Information security questions, 2019, 2(125), P. 36–40. URL:http://izdat.ntckompas.ru/editions/for_readers/archive/article_detail.php?SECTION_ID=155&ELEMENT_ID=24535 (accessed: 20.02.2020) (in Russian).
[12] Solodjannikov A.V. Organizacija i upravlenie sluzhboj zashhity informacii / A.V. Solodjannikov. – SPb.: Sankt-Peterburgskij gosudarstvennyj jekonomicheskij universitet, 2018. – 89 s. URL: https://elibrary.ru/item.asp?id=37310180 (accessed: 20.02.2020) (in Russian).

[13] Mustafaev V.A., Salmanova M.N. Modeling dynamic interaction processes using fuzzy petri nets of V_F type. Bulletin of Voronezh state technical University. 2019. Vol. 15. No 3. P. 28–33. DOI: 10.25987/VSTU.2019.15.3.004. URL: https://cchgeu.ru/science/nauchnye-izdaniya/vestnik-voronezhskogo-gosudarstvennogo-tekhnicheskogo-universiteta-/fayly/vypuski/15_3.pdf (accessed: 20.02.2020) (in Russian).

[14] Zaitsev D.A., Shmeleva T.R., Groote J.F. Verification of Hypertorus Communication Grids by Infinite Petri Nets and Process Algebra. IEEE/CAA Journal of Automatica Sinica, 6(3), 2019, 733–742. DOI: 10.1109/JAS.2019.1911486. URL: https://ieeexplore.ieee.org/document/8707130 (accessed: 20.02.2020).

[15] Chucklyaev I.I. Methodical Providing Complex Management of Risks of Informational Security of Function-Oriented Information Resources Management Information Systems. Voprosy kiberbezopasnosti, 2016, 4(17). P. 61–71. URL: https://elibrary.ru/item.asp?id=27441076 (accessed: 20.02.2020) (in Russian).

Поступила в редакцию – 29 февраля 2020 г. Окончательный вариант – 22 мая 2020 г.
Received – February 29, 2020. The final version – May 22, 2020.