УДК 004.942 DOI: 10.17587/it.25.757-765

В. Н. Костин, канд. тех. наук, доц., e-mail:vladimirkostin5@mail.ru,
Федеральное государственное бюджетное образовательное учреждение высшего образования
"Оренбургский государственный университет"

Оценка эффективности физической защиты информации критически важных объектов на основе марковских цепей

Разработан метод моделирования оценки эффективности физической защиты информации критически важных объектов. Особенностью решения задачи является декомпозиция сложного мультиграфа проникновения нарушителя к информационным ресурсам объекта на множество простых графов, каждый из которых представлен в виде последовательности событий. Иными словами, осуществляется декомпозиция сложной задачи на множество простых подзадач. Результат декомпозиции представлялся в виде матрицы инцидентности: строки — номер пути проникновения, столбцы — ребра графа проникновения нарушителем. Каждый путь нарушителя и реакция физической защиты на проникновение моделируются двумя информационно связанными марковскими цепями. Показателем эффективности физической защиты выбрана вероятность защиты информации. Система оценки защищенности состоит из дизъюнктивно связанных путей проникновения, при этом каждый путь — это набор конъюнктивно связанных ребер проникновения, который определяется вероятностью реализации цели нарушителя. Общая оценка физической защиты информации проводится по самому пессимистическому пути проникновения нарушителя.

Ключевые слова: *оценка эффективности физической защиты, мультиграф проникновения нарушителя, матрица инцидентности*

Введение

В условиях возрастающих угроз (развития терроризма) и повышения возможностей современных технологий задача оценки эффективности физической защиты (ФЗ) информации становится все более актуальной. Это связано, в первую очередь, с возрастающей сложностью систем защиты. Кроме того, среди последовательных этапов проектирования ФЗ завершающим и важным этапом разработки является оценка ее эффективности.

Вопросам оценки эффективности ФЗ посвящено много статей, в которых рассматриваются несколько подходов к оценке эффективности. Например, А. В. Леус в статье [1] предлагает показатели оценки эффективности ФЗ и математическую модель на основе трехмерного куба. Достоинство метода: при оценке вероятности безопасного состояния используется логарифмическая функция, позволяющая перейти к сложению показателей защищенности объекта. Это удобно при анализе эффективности ФЗ. Недостатком метода является большая многомерность задачи из-за бесконечного множества точек пространства движения нарушителя. С. И. Корчагин в статье [2] предлагает методику оценки ФЗ с помощью вероятностного подхода, достоинством которой является тот факт, что в модели осуществляется переход к одномерной структуре комплекса, за счет чего упрощаются расчеты оценки эффективности ФЗ. Однако в данной методике нет обоснования значения порога вероятности для перехода к одномерной структуре комплекса. С. С. Звежинский и др. в статье [3] рассматривают эффективность охранной сигнализации для малых объектов, при этом учитывают важность критических элементов путем введения коэффициента важности в целевую функцию оценки рационального расположения технических средств защиты (ТСЗ) на рубежах охраны. Недостатком является решение задачи без ограничений. Кроме того, многие методы оценки эффективности ФЗ основаны исключительно на экспертных оценках, что привно-

сит элемент субъективизма в оценку, а также зависимость от знаний и опыта экспертов.

Оценка эффективности ФЗ с использованием логико-вероятностных методов (ЛВМ) рассматривается в статьях О. А. Панина [4, 5], где делается акцент на большую трудоемкость ЛВМ. Полученные результаты комплексной оценки ФЗ по данной методике [5, 6] при большом числе вариантов проникновения занижают показатель защищенности системы защиты.

Проведенный в монографии [7] анализ показателей и методов оценки эффективности ФЗ показал, что не существует универсальных методик оценки эффективности ФЗ. На сегодняшний день применяется несколько методик оценки эффективности ФЗ: детерминистический подход; логико-вероятностный метод; вероятностно-временной метод. При детерминистическом подходе за эффективность принимается степень выполнения требований по физической защите в соответствии с нормативными документами. Предполагается проведение комплекса проверок требований, содержащихся в руководящих документах. Для каждого фактора состояния разрабатывается аналитическая модель для оценки организационных мероприятий. В логико-вероятностном методе под эффективностью понимается вероятность нахождения системы в безопасном состоянии согласно построенному сценарию развития опасной ситуации. Составленная функция опасности системы в виде логического многочлена заменяется на вероятностный многочлен для определения показателя системы — вероятности наступления опасного события. При вероятностно временном методе под эффективностью понимается вероятность того, что у сил реагирования резерв времени окажется больше нуля, т. е. ФЗ успешно выполнила функцию. Для этого проводится оценка всех маршрутов движения нарушителя и реагирования группы нейтрализации.

Материал данной статьи является продолжением исследований вопросов оценки эффективности ФЗ на основе методов системного анализа.

Постановка задачи

Для оценки функционирования ФЗ необходимо определить показатель эффективности. По мнению авторов работы [7], наиболее полно характеризующим показателем эффективности функционирования ФЗ является вероятность нахождения информации критически важного объекта (КВО) в безопасном состоянии. Данный показатель определяется двумя связанными показателями: вероятностью обнаружения нарушителя и вероятностью своевременного прибытия сил охраны для нейтрализации нарушителя:

$$P(V) = P(A)P(R/A)P(V/(R/A)), \qquad (1)$$

где $P(A)$ — вероятность получения силами охраны сигнала тревоги; $P(R/A)$ — вероятность развертывания сил охраны в точке перехвата при условии уверенного приема сигнала тревоги; $P(V/(R/A))$ — вероятность нейтрализации нарушителя при условии своевременного развертывания сил охраны. Данный показатель не исследуется — принимается за единицу.

Целью настоящих исследований является разработка метода оценки эффективности ФЗ (оценки варианта размещения ТСЗ) на основе синтеза марковских цепей. Для решения этой задачи необходимо разработать метод формирования логических функций проникновения, на основе которых осуществляется оценка эффективности ФЗ.

Разработанный метод позволяет получить совокупность всех путей проникновения нарушителя к информационным ресурсам объекта, представленных как логические функции проникновения в виде дизъюнкции и конъюнкции логических переменных — ребер графа, которые сформированы в информационную матрицу инцидентности для решения задачи оценки эффективности ФЗ.

Достоинства метода: 1) сложная задача оценки вероятности безопасного состояния информации представлена как оценка надежности системы в виде мультиграфа, который декомпозируется на множество простых графов проникновения нарушителя; 2) входные данные в модель оценки вероятности проникновения нарушителя формируются с помощью проведения натурного эксперимента на объекте защиты, что повышает их точность и, как следствие, достоверность оценки показателя эффективности ФЗ.

Решение задачи рассмотрим на модельном примере. КВО представляет собой сложную систему, состоящую из множества связанных зон охраны различной природы назначения, важности и уровня защищенности (рис. 1). Вся территория объекта имеет двойное ограждение, периметровую охрану и контрольно пропускной пункт (КПП). На КВО имеется элемент информатизации (ЭИ), подлежащий охране. На рубежах зон охраны располагаются

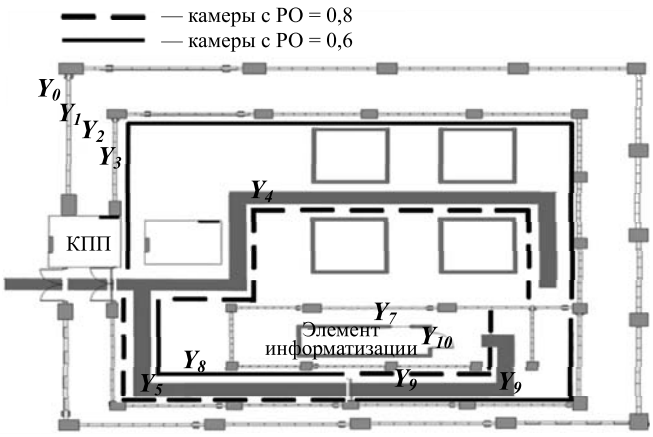

Рис. 1. Расположение ТСЗ (камер видеонаблюдения) на объекте

ТСЗ. Цель нарушителя — проникнуть в ЭИ и совершить хищение информации. Модель проникновения нарушителя представлена в виде разветвленного ориентированного мультиграфа (рис. 2). Мультиграф — это сценарий проникновения нарушителя на охраняемый объект. Вершинами графа являются рубежи зон охраны при достижении нарушителем определенного результата на пути к цели. Ребра графа — это варианты перемещений нарушителя между рубежами охраны. Ребра обозначены X_i, где i — номер ребра (варианта перемещения) в графе. Всего определим n рубежей зон охраны. Следовательно, граф имеет n вершин (событий). Первая вершина — Y_0, последняя Y_n. Событию Y_0 присваивается единица, т. е. это вероятность нахождения нарушителя в нулевом событии в начальный момент времени. Наступление события Y_n означает факт проникновения нарушителя к информационным ресурсам (нарушитель достиг цели (произошло хищение и т. д.)). Вероятность нахождения события Y_n в безопасном состоянии и будет показателем эффективности ФЗ.

На рис. 2 обозначено: X_1 — преодоление первого ограждения через верх; X_2 — преодоление ограждения путем разрушения ограждения; X_3 — подкоп первого ограждения; X_4 — вариант перемещения зоны бегом; X_5 — преодоление зоны ползком; X_6 — преодоление второго ограждения через верх; X_7 — разрушение второго ограждения; X_8 — подкоп второго ограждения; X_9 — проход через КПП путем подбора ПИН-кода; X_{10} — проникновение через ворота путем подмены документов; $X_{11}...X_{21}$ — варианты перемещения через зоны между рубежами Y_{3-10} внутри объекта (см. рис. 1).

Для отображения противодействия ФЗ введем еще один ориентированный граф (рис. 3). Вершины графа обозначают рубежи противодействия системы защиты от нарушителя. Ребро в графе ассоциируется с каким-то типом варианта защиты объекта, который будет характеризоваться вероятностью защиты, т. е. ребро — вероятность того, что ФЗ обнаружит нарушителя и окажет противодействие при переходе между рубежами. Ребра также будем обозначать Z_i, где i — номер ребра (вариант противодействия) в графе.

Полученный граф назовем графом противодействия. Всего будем определять n рубежей, как и в предыдущем графе, т. е. граф имеет n вершин. Первая вершина — Y_n, последняя — Y_0. Событию Y_n присваивается значение 1. Ребра будут направлены от вершины Y_n к Y_0.

Марковская модель позволяет оценить вероятности состояний двух противоборствующих

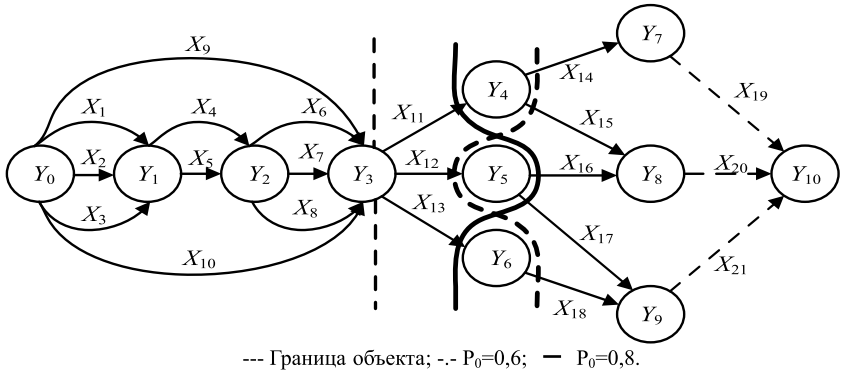

Рис. 2. Граф достижимости нарушителем цели

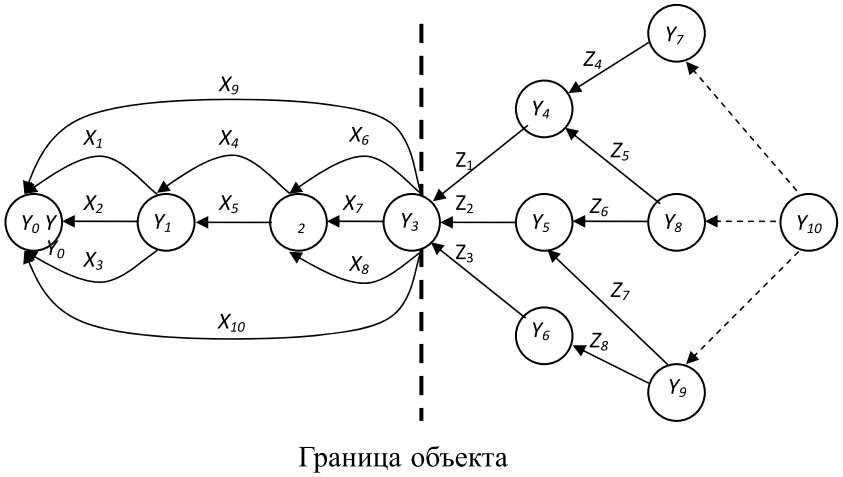

Рис. 3. Граф противодействия ФЗ проникновению нарушителя

систем: нарушителя и ФЗ, т. е. оценить вероятность реализации угрозы. Исходными данными является вектор начальных состояний нарушителя, матрица смежности вероятностей преодоления рубежей защиты за время Δt и матрица смежности вероятностей противодействия (нейтрализации нарушителя) ФЗ. Исходные данные определяются расчетным путем и методом экспертных оценок, а также проведением натурного эксперимента на физическом объекте защиты. В процессе моделирования определяется вектор предельных вероятностей состояний каждого события графа (рубежа) — вероятность безопасного состояния объекта.

Таким образом, имеем марковскую модель с дискретными состояниями, представленную в виде ориентированного взвешенного графа. Переход системы из состояния в состояние будем рассматривать в дискретные моменты времени Δt. Система считается заданной, если заданы два условия: 1 — вероятность начальных состояний системы $Pi(t)$ вектором $P_i^{(0)} = (P_{01}, P_{02}, \ldots, P_{0n})$; 2 — условные вероятности переходов $Pik(\Delta t)$ из i-го в k-е состояние за время Δt:

$$P_{ik}(\Delta t) = \begin{vmatrix} P_{11}(\Delta t) & P_{12}(\Delta t) & \ldots & P_{1n}(\Delta t) \\ \ldots & \ldots & \ldots & \ldots \\ P_{n1}(\Delta t) & P_{n2}(\Delta t) & \ldots & P_{nn}(\Delta t) \end{vmatrix}. \quad (2)$$

Тогда вероятность нахождения системы в k-м состоянии в момент времени $t + \Delta t$ будет определяться по формуле полной вероятности:

$$P_k(t + \Delta t) = P_1(t)P_{1k}(\Delta t) + P_2(t)P_{2k}(\Delta t) + \ldots + P_k(t)P_{kk}(\Delta t) + \ldots + P_n(t)P_{nk}(\Delta t), \quad (3)$$

или в матричном виде данное выражение можно записать в следующем виде:

$$P(t + \Delta t) = P(t)P_{ij}(t + \Delta t), \quad (4)$$

где $P(t) = \{P_1(t), P_2(t), \ldots, P_n(t)\}$ — вектор начальных состояний; P_{ij}:$\{P_{ij}\}$, i, j:1...n — матрица вероятностей переходов системы.

Для однородной цепи Маркова вероятности переходов из i-го в j-е состояние во времени можно записать в виде:

$$P_{ij}(t, t + m\Delta t) = P_{ij}^m(t, t + \Delta t). \quad (5)$$

Поэтому для однородной цепи Маркова существует эргодическое свойство, суть которого состоит в том, что система в пределе переходит к установившемуся состоянию:

$$\lim_{m\to\infty} P_i(t + m\Delta t) = P_i^*, \quad (6)$$

где P_i^* — предельные (финальные) вероятности.

К моменту времени $t + m\Delta t$ вероятности состояний системы двух шагов $m - 1$, m практически равны между собой. Тогда из уравнения Маркова получим вероятность k-го события:

$$P_k = \sum_{i=1}^{n} P_i P_{ik}. \quad (7)$$

Добавляется требование нормировки:

$$\sum_{i=1}^{n} P_i = 1. \quad (8)$$

Поскольку математический аппарат марковских моделей не позволяет описывать мультиграф, поэтому путем стягивания весов ребер к одному ребру перешли к обычному графу. Так как граф достижимости нарушителем цели и граф противодействия отличаются только направлением дуг, то графы можно совместить, при этом матрица смежности вероятностей переходов между вершинами за время Δt результирующего графа получится путем объединения матриц смежности исходных графов с нормированием вероятностей переходов (рис. 4).

Ребра, показанные сплошными линиями, обозначают вероятности переходов нарушителя между рубежами за время Δt, а ребра, показанные штриховыми линиями, — вероятности противодействия ФЗ проникновению. Вектор

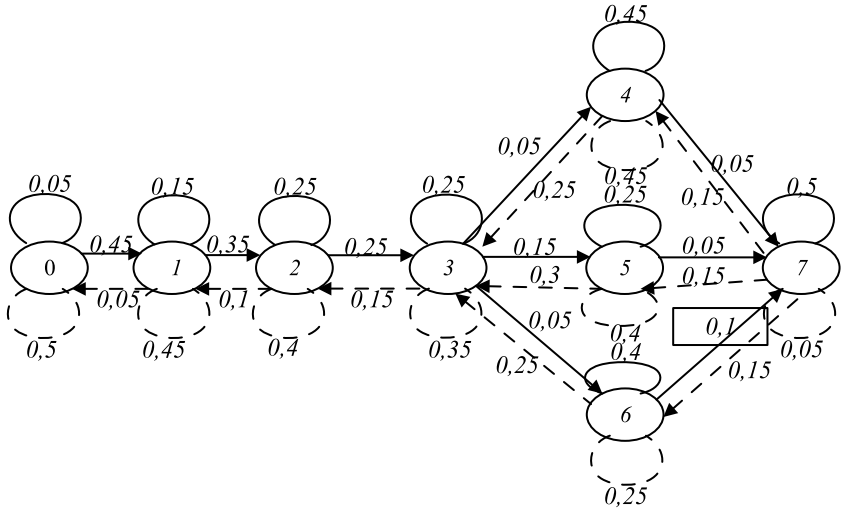

Рис. 4. Граф проникновения нарушителя и противодействия ФЗ

Таблица 1

Матрица инцидентности

№ функции проникновения	Номера ребер графа																				
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}
1									1		1			1					1		
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
100			1		1			1					1					1			1

исходного состояния нарушителя представлен в виде вектора-строки. Умножая вектор вероятности состояний на матрицу смежности вероятностей, получаем установившийся результат на определенной итерации. Вероятность конечного n-го события и будет вероятностью безопасного состояния информации. С использованием данных теоретических предпосылок было разработано программное средство на языке программирования C#, реализующее оценку эффективности ФЗ.

Решение задачи оценки эффективности с помощью марковской модели в такой постановке составило непреодолимую трудность по следующим причинам: большая размерность задачи, сложность проведения нормировки графа при взаимодействии противодействующих сторон и трудности принятия решений, направленных на повышение эффективности ФЗ. По этой причине перешли к синтезу марковских цепей оценки эффективности ФЗ.

Для этого проводили декомпозицию мультиграфа проникновения нарушителя. Определяли все пути перемещений из начальной вершины Y_0 в конечную Y_{10}. Все варианты пути из одной смежной вершины в другую обозначили как дизъюнкцию логических переменных. Например, перемещение из вершины Y_0 в вершину Y_1 будем обозначать $X_1 \vee X_2 \vee X_3$.

Пути из одной вершины в другую определяли с помощью операции композиции матрицы смежности мультиграфа. Чтобы найти пути, состоящие из k ребер, необходимо возвести матрицу смежности в степень k. При этом получим новую матрицу, в которой будут представлены все пути между событиями длиной от одного ребра до k ребер. Таким образом, в полученной логической функции проникновения параллельные маршруты будут представлены как дизъюнкции ребер, а последовательные — как их конъюнкции. Также следует учесть, что умножаемые матрицы смежности содержат логические переменные. Из этого следует, что к результатам умножения ячеек можно применить операции алгебры логики для сокращения результата умножения [6]: 1) правила для одной переменной $A \vee 1 = 1$; $A \vee 0 = A$; 2) закон тавтологии $A \vee A \vee ...A = A$; — $A \wedge A \wedge ...A = A$; 3) распределительный закон — $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$.

Используя данные теоретические предпосылки, определим все возможные пути из первого рубежа в последний, представленные как функции алгебры логики в виде конъюнкции весов ребер, по которым проходит путь. Для удобства операцию конъюнкции переменных $X_1 \wedge X_2$ будем обозначать X_1X_2, а операцию дизъюнкции $X_1 \vee X_2$ будем обозначать $X_1 + X_2$. Всего получили 100 логических функций проникновения нарушителя, из которых десять имеют длину в четыре ребра, а девяносто — длиной в шесть ребер. Полученные функции алгебры логики сведены в матрицу инцидентности (табл. 1): строки в матрице — маршруты проникновения (функции), а столбцы — ребра графа между рубежами объекта, на которых расположены ТСЗ с характеристиками (табл. 2).

Элементы матрицы инцидентности в строке связаны конъюнктивно, а сами строки — дизъюнктивно. Полученные логические функции проникновения позволяют оценить вероятность проникновения и противодействия на каждом маршруте, т. е. оценить эффективность ФЗ. В вероятностном смысле эффективность ФЗ будет определяться вероятностью нереализации ни одной из ста функций проникновения.

С точки зрения системного анализа процесс получения всех путей проникновения (функций проникновения) — это декомпозиция сложной задачи на более простые подзадачи.

Таблица 2

Характеристики технических средств защиты

Тип ТСЗ	Расположение на графе проникновения	P обнаружения	Протяженность, м	Удаление от ЭИ, м
CNB-WFL-21S	X_{11}, X_{16}, X_{17}, X_{13}	0,60	880	450
SCANALL	X_{12}, X_{14}, X_{15}, X_{18}	0,80	670	300

После этого согласно теории системного анализа решается задача синтеза и оценки эффективности ФЗ.

Вероятности обнаружения и перехвата (своевременного прибытия для нейтрализации) нарушителя обоснованы и заданы на предыдущих этапах проектирования ФЗ [9]. Определим требования к ФЗ: вероятность обнаружения нарушителя на каждом пути проникновения не менее 0,9; вероятность своевременного прибытия в точку пресечения группы реагирования на каждом пути не менее 0,8, т. е. вероятность безопасного состояния объекта $P_{бс}$ не меньше 0,72.

На основе длин ребер на местности определим протяженность пути проникновения как их сумма в соответствии с табл. 1: X_1 — 25 м; X_2 — 15 м; X_3 — 35 м; X_4 — 14 м; X_5 — 24 м; X_6 — 20 м; X_7 — 15 м; X_8 — 24 м; X_9 и X_{10} — 13 м; X_{11} — перемещение между рубежами Y_3—Y_4 — 450 м; X_{12} — перемещение между рубежами Y_3—Y_5 — 320 м; X_{13} — между рубежами Y_3—Y_6 — 220 м; X_{14} — между рубежами Y_4—Y_7 — 180 м; X_{15} — между рубежами Y_4—Y_8 — 50 м; X_{16} — между рубежами Y_5—Y_8 — 160 м; X_{17} — между рубежами Y_5—Y_9 — 50 м; X_{18} — между рубежами Y_6—Y_9 — 120 м; X_{19} — между рубежами Y_7—Y_{10} — 60 м; X_{20} — между рубежами Y_8—Y_{10} — 70 м; X_{21} — между рубежами Y_9—Y_{10} — 50 м. Расстояние от караула до ЭИ — 310 м.

Для решения задачи оценки вероятности проникновения нарушителя по порядку моделировали все пути проникновения из матрицы инцидентности (см. табл. 1) в виде последовательных событий перемещения нарушителя между рубежами охраны и противодействия проникновению сил охраны. Данная последовательность описывалась двумя простыми связанными моделями: первая модель — модель перемещения нарушителя, вторая — модель перемещения группы нейтрализации нарушителя после его обнаружения. Обе модели описываются с помощью последовательного графа переходов событий. Модели взаимосвязаны и работают синхронно. Процесс движения $x(t)$ считаем как поток независимых приращений расстояний с интенсивностью (скоростью) $\lambda(t)$. Так как приращения на любом участке времени t, $t + \Delta t$ независимы, то процесс приращения расстояния при движения $x(t)$ является пуассоновским процессом с ограниченным числом состояний $x(t) \leqslant L$, где L — расстояние между событиями [9]. Вероятности переходов между событиями за время Δt определяются по экспоненциальному закону исходя из значения скорости перемещения между рубежами охраны. Графы проникновения и противодействия представлены на рис. 5.

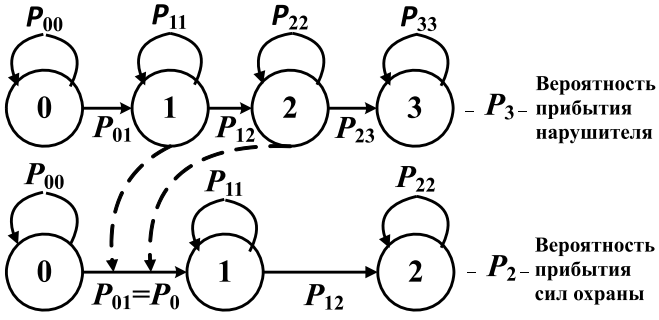

Рис. 5. Синхронизация графов проникновения и противодействия ФЗ

Вершины графов — рубежи перемещений через зоны охраны нарушителя и группы нейтрализации. Особенностью второго графа переходов является то, что он информационно связан с первым графом (на рис. 5 это показано штриховыми ребрами). Матрица вероятностей переходов изменяется динамически, в зависимости от вероятности состояния событий (1) и (2) модели движения нарушителя. Таким образом, марковская модель реакции группы нейтрализации на проникновение нарушителя не стационарна. По мере перемещения нарушителя вероятность состояний (1) и (2) увеличивается и, следовательно, увеличивается вероятность обнаружения. Из состояний (1) и (2), где находятся средства технического контроля, информация передается в ребро 0 — 1 на второй марковский граф в виде вероятности обнаружения, т. е. содержание матрицы переходов вероятностей динамически изменяется. Эта информация в виде возрастающей вероятности передается во второй граф (матрицу переходов), и, следовательно, вероятность начала перемещения группы нейтрализации увеличивается. Во второй модели графа группы нейтрализации переход из нулевого состояния в первое состояние — это и есть вероятность обнаружения нарушителя ТСЗ в виде логической связи. Таким образом, движение группы нейтрализации начинается с первого события при получении информации (обнаружении нарушителя) с двух рубежей расположения технических средств обнаружения. Последние вершины обоих графов имеют одно и то же физическое положение на местности — ЭИ.

Вероятность перехода из нулевого события в первое (вероятность обнаружения) определяется по формуле умножения вероятностей последовательных событий, так как наруши-

тель последовательно пересекает рубежи, на которых расположены ТСЗ. Результирующее действие оценивает вероятность перехода на графе из нулевого события в первое, как произведение вероятностей не обнаружения на каждом рубеже:

$$P_{01} = 1 - [(1 - P^1_{\text{ТСЗ}} P_1)(1 - P^2_{\text{ТСЗ}} P_2)], \qquad (9)$$

где $P^1_{\text{ТСЗ}}$, $P^2_{\text{ТСЗ}}$ — вероятности обнаружения ТСЗ, расположенных на графе в вершинах событий 1 и 2 соответственно;

P_1, P_2 — вероятности нахождения нарушителя в зоне обнаружения ТСЗ на рубежах событий вершин графа проникновения 1 и 2 соответственно.

Функционирование графов синхронизировано по времени с шагом продолжительности $\Delta t = 1$ с. В результате моделирования определяли значения вероятности обнаружения, которые передавали во вторую модель противодействия. Во второй модели на графе с помощью марковской модели графа определяется вероятность своевременного прибытия группы нейтрализации, т. е. вероятность наступления события (2).

Выходными значениями марковских моделей являются вероятности наступления конечных событий, т. е. реализация целей нарушителя и группы нейтрализации. Полученные графики изменения вероятностей конечных событий сравниваются, и проводится анализ выходной информации. По соотношению вероятностей конечных событий можно сделать вывод о безопасном состоянии объекта [10].

Процесс моделирования автоматизирован с помощью программы на языке программирования C#. Исходные данные представлены в виде характеристик: расстояния и скорости движения противоборствующих сторон в соответствующих зонах охраны. Результаты решения и динамика изменения вероятности состояний конечных событий представлены на рис. 6, 7.

Достоверность результатов определяется корректностью задаваемых входных матриц вероятности переходов. Данные вероятности определяются расчетным путем и согласовываются с экспериментальными данными [12] как элемент вероятности: $\Delta P_{ij} = \lambda_{ij} \Delta t$, где λ_{ij} — интенсивность (скорость) движения нарушителя между рубежами и сил охраны к месту расположения ЭИ.

Оценка вероятности нахождения объекта в безопасном состоянии по вероятностям двух конечных событий определяется по формуле гипотез. Оценивается первая гипотеза, состоящая в том, что группа нейтрализации опередит нарушителя, и вторая гипотеза, что нарушитель опередит группу нейтрализации. Условная вероятность появления первой гипотезы определялась по формуле [12, стр. 64]

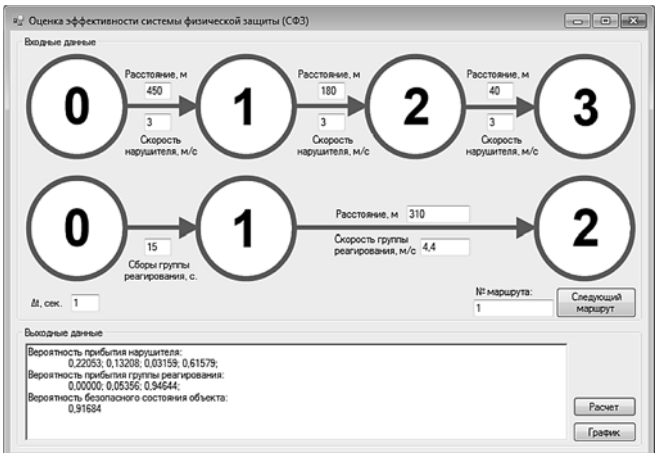

Рис. 6. Входные данные и результаты вычислений

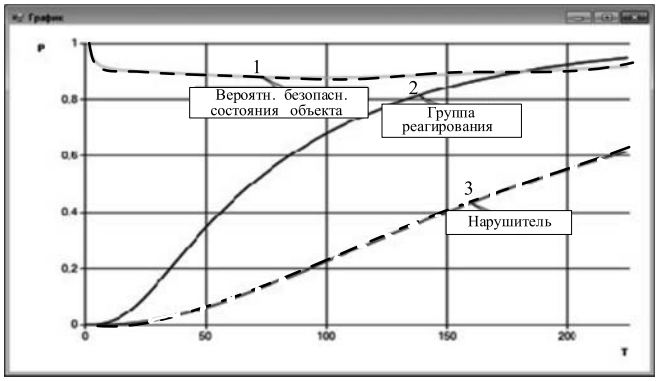

Рис. 7. Динамика изменения вероятности конечных событий

$$P(H_1/A) = PH_1/(PH_1 + PH_2), \qquad (10)$$

где $PH_1 = P_1(1 - P_2)$ — вероятность первой гипотезы; $PH_2 = (1 - P_1)P_2$ — вероятность второй гипотезы; P_1, P_2 — вероятности прибытия к месту развертывания группы нейтрализации и нарушителя соответственно.

Данная задача решается для каждого из ста маршрутов проникновения матрицы инцидентности (см. табл. 1). В результате анализа всех путей проникновения с учетом расположения ТСЗ получили матрицу инцидентности, содержащую всего пять уникальных функций проникновения до границы объекта (табл. 3).

Результаты вычислений вероятностей безопасного состояния сведены в табл. 4.

Анализ табл. 4 показывает, что требования к эффективности ФЗ выполнены [9]. Про-

Таблица 3

Инцидентности уникальных маршрутов в границах объекта

№ функции проникновения	Номер дуги графа										
	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}
1	1			1					1		
2	1				1					1	
3		1				1				1	
4		1					1				1
5			1					1			1

Таблица 4

Результаты моделирования марковских процессов

№ функции проникновения	Вероятность прибытия сил охраны PH_1	Вероятность прибытия нарушителя PH_2	Вероятность безопасного состояния объекта $P(H_1/A)$
1	0,951	0,615	0,924
2	0,912	0,633	0,857
3	0,912	0,608	0,870
4	0,837	0,635	0,747
5	0,815	0,612	0,736

граммное средство адекватно реагирует на вводимые изменения в структуру модели, что говорит о чувствительности модели к входным данным.

Заключение

Разработанный метод на основе синтеза марковских цепей позволяет оценить эффективность функционирования ФЗ. Применение разработанного математического аппарата автоматизировано. Программное средство адекватно реагирует на вводимые в структуру модели изменения, что говорит о чувствительности модели к входным данным. Результатами моделирования являются вероятности безопасного состояния ЭИ при попытке нарушителя проникнуть на объект по каждому маршруту. На каждом пути проникновения обеспечивается безопасное состояние объекта на уровне не меньше заданных требований.

Достоинством разработанного метода моделирования является тот факт, что повышается достоверность результатов оценки из-за возможности детализировать маршрут проникновения нарушителя и, получив множество разнородных по сложности участков, корректно задавать входные данные по скорости преодоления этих участков, определяя их экспертным путем и согласовывая с экспериментальными данными натурного эксперимента на реальном объекте.

Список литературы

1. **Леус А. В.** Математическая модель оценки эффективности систем физической защиты // T-Comm — Телекоммуникации и Транспорт. 2010. № 6. С. 46—49.

2. **Корчагин С. И.** Оценка эффективности ИК ФЗ в рамках вероятностного подхода // T-Comm — Телекоммуникации и Транспорт. 2010. № 4. С. 46—47.

3. **Звежинский С. С., Голубков Г. В., Иванов В. А.** Оценка функциональной эффективности охранной сигнализации малых объектов // Спецтехника и связь. 2008. № 3. С. 13—20.

4. **Панин О. А.** Проблемы оценки эффективности функционирования систем физической защиты объектов // Безопасность, достоверность информация (БДИ). 2005. № 3. С. 22—27.

5. **Панин О. А.** Как измерить эффективность // БДИ. 2008. С. 20—24.

6. **Рябинин И. А.** Надежность и безопасность структурно-сложных систем. СПб.: Изд-во СПбГУ, 2007. 276 с.

7. **Боровский А. С., Тарасов А. Д.** Автоматизированное проектирование и оценка систем физической защиты потенциально — опасных (структурно-сложных) объектов. Часть 1: Системный анализ проблемы проектирования и оценки систем физической защиты. Самара; Оренбург: Сам ГУПС, ОрИПС — филиал Сам ГУПС, 2012. 163 с.

8. **Рекомендации** по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. ФСТЭК России, 2007 г.

9. **Мишин Е. Т., Соколов Е. Е.** Построение систем физической защиты потенциально опасных объектов. М.: Радио и связь, 2005. 200 с.

10. **Вентцель Е. С., Овчаров Л. А.** Теория случайных процессов и ее инженерные приложения. М.: Высшая школа, 2003. 432 с.

11. **Вентцель Е. С.** Теория вероятностей. М: Наука, 2013. 368 с.

12. **Никитин В. В., Цицулин А. К.** Телевидение в системах физической защиты. URL: https://www.security-bridge.com/ (дата обращения 13.10.2005).

V. N. Kostin, Cand. Tech. Sci., Associate Professor, e-mail: vladimirkostin5@mail.ru,
Federal State Educational Government-financed Institution
of Higher Professional Education "Orenburg State University"

Assessment of Efficiency of Physical Security of Information of Crucial Objects on the Basis of Markov Chains

The method of modeling of assessment of efficiency of physical security of information of crucial objects is developed. Feature of the solution of a task is decomposition of a complicated multigraph of penetration of the violator to information resources of an object on a great number of ordinary graphs, each of which is presented in the form of the sequence of events. This is decomposition of a difficult task on a set of simple subtasks. The result of decomposition was presented in the incidence matrix form: lines — number of a way of penetration, columns — edges of the graph of penetration by the violator. Every way of the violator and reaction of physical protection to penetration is modelled by two information-related Markov chains. Probability of information security is chosen as an indicator of efficiency of physical protection. The system of assessment of security consists of disjuctive-connected ways of penetration, at the same time every way it is a set conjuctive-connected edges of penetration which is defined by the probability of realization of the purpose of the violator. The general assessment of physical security of information is made on the most pessimistic way of penetration of the violator.

Keywords: *assessment of efficiency of physical protection, multigraph of penetration of the violator, incidence matrix*

DOI: 10.17587/it.25.757-765

References

1. **Leus A. V.** *T-Comm — Telekommunikacii i Transport*, 2010, no. 6, pp. 46—49 (in Russian).
2. **Korchagin S. I.** *T-Comm — Telekommunikacii i Transport*, 2010, no.10, pp. 46—47 (in Russian).
3. **Zvezhinskij S. S., Golubkov G. V., Ivanov V. A.** *Spectekhnika i Svyaz'*, 2008, no. 3, pp. 13—20 (in Russian).
4. **Panin O. A.** *Bezopasnost', dostovernost' informaciya (BDI)*, 2005, no. 3, pp. 22—27 (in Russian).
5. **Panin O. A.** *Bezopasnost', dostovernost' informaciya (BDI),* 2008, no. 2, pp. 20—24 (in Russian).
6. **Ryabinin I. A.** Reliability and safety of structurally complex systems, SPb, Publishing house of SPbGU, 2007, 276 p. (in Russian).
7. **Borovskij A. S., Tarasov A. D.** Computer-aided design and assessment of physical protection systems for potentially dangerous (structurally complex) objects. Part 1: System analysis of the problem of designing and evaluating physical protection systems, Samara; Orenburg, Sam GUPS, OrIPS—filial Sam GUPS, 2012, 163 p. (in Russian).
8. **Recommendations** for ensuring information security in key systems of information infrastructure, FSTEK Rossii, 2007 g. (in Russian).
9. **Mishin E. T., Sokolov E. E.** Construction of physical protection systems for potentially dangerous objects, Moscow, Radio i svyaz', 2005, 200 p. (in Russian).
10. **Ventcel' E. S., Ovcharov L. A.** The theory of random processes and its engineering applications, Moscow, 2003, 432 p. (in Russian).
11. **Ventcel' E. S.** Probability theory, Moscow, Nauka, 2013, 368 p. (in Russian).
12. **Nikitin V. V., Ciculin A. K.** Television in physical protection systems, available at: https://www.security-bridge.com/ (date of access 13.10.2005) (in Russian).