Уфа : УГАТУ, 2007 Вестник УГАТУ • Управление, ВТ и И Т. 9, № 7 (25). С. 11–19

УДК 519.8:658

Т. О. ВИШНЯКОВА, В. И. ВАСИЛЬЕВ

АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ПРИ ПОМОЩИ МАРКОВСКОЙ СЕТЕВОЙ МОДЕЛИ

Рассматривается актуальная проблема моделирования систем физической защиты. Рассмотрены структура и функции систем физической защиты, а также показатели их работы. Рассмотрен программный продукт для оценки показателей риска на основе марковской сетевой модели системы физической защиты. Затронут вопрос практического применения предложенных разработок на примере административного здания. *Риск; среднеожидаемый ущерб; марковская сеть; система физической защиты; моделирование*

ВВЕДЕНИЕ

На сегодняшний день актуальной задачей является задача проектирования комплексных систем защиты информации. К сожалению, на практике она решается только на основе опыта и преимущественно без должного математического обоснования выбираемых решений [1].

Комплексная безопасность информационных систем включает в себя следующие составляющие:

- физическая безопасность (защита зданий, помещений, подвижных средств, людей, а также аппаратных средств — компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
- безопасность связи (защита каналов связи от внешних воздействий любого рода);
- безопасность программного обеспечения (защита от вирусов, логических бомб, несанкционированного изменения конфигурации);
- безопасность данных (обеспечение конфиденциальности, целостности и доступности данных).

Так сложилось, что хронологически первой стала развиваться физическая безопасность, а уже потом — другие разделы информационной безопасности [2].

СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ И ЕЕ СТРУКТУРА

Система физической защиты (СФЗ) — совокупность персонала физической защиты, осуществляемых им организационно-технических мероприятий и действий, а также инженерно-технических средств, предназначенная для реализации физической защиты [3].

В этом едином комплексе, который представляет собой система физической защиты, задействованы люди (служба безопасности, силы охраны), и техника — комплекс инженерно-технических средств охраны (ИТСО) или комплекс инженерно-технических средств физической защиты (ИТСФЗ). От их четкого взаимодействия зависит эффективность СФЗ.

Современные СФЗ строятся на базе широкого применения инженерно-технических и программных средств и содержат следующие основные составные части (подсистемы) [4]:

- система контроля и управления доступом персонала (СКУД),
- система охранной сигнализации (СОС),
- система телевизионного наблюдения (СТН),
- система оперативной связи и оповещения,
- обеспечивающие системы (освещения, электропитания и др.).

При создании современных СФЗ, как правило, ставится также и задача защиты жизненно важных центров и систем объекта от непреднамеренных, ошибочных или некомпетентных действий персонала, которые по характеру возможного ущерба приближаются к НСД внешних нарушителей [4].

Определенный уровень безопасности объекта может быть достигнут различными способами, например, путем использования мно-

гочисленного штата сотрудников охранных структур или установки нескольких автономных технических систем безопасности (ТСБ) разного типа [5].

ФУНКЦИИ СФЗ

Хищения и диверсии на территории объекта могут быть предотвращены двумя способами — удержанием нарушителей от совершения этих действий или успешным противодействием нарушителям.

Удержание обеспечивается внедрением СФЗ, которую потенциальные нарушители рассматривают как непреодолимое препятствие. Под непреодолимостью следует понимать не только невозможность преодоления высоких заборов, но и неминуемость обнаружения нарушителей техническими средствами, в том числе аппаратурой видеонаблюдения. В частности, для реализации функции удержания в состав ТВ-систем для СФЗ кроме обычных и скрытно установленных телекамер иногда вводят их муляжи. Связанная с методами удержания проблема состоит в том, что измерить эффективность удержания численно невозможно.

Противодействие нарушителям предусматривает определенные мероприятия сил охраны, предотвращающие хищение или диверсию после начала фактических действий нарушителей. Существует несколько функций, которые должна выполнять система физической защиты. Для оценки всей системы в целом необходимо исчерпывающее понимание определений этих функций и возможность количественной оценки эффективности их выполнения.

К основным функциям СФЗ относятся [6]:

- обнаружение:

— обнаружение вторжения техническими средствами,

— обеспечение связи средств обнаружения с силами охраны,

— оценка тревожной ситуации;

- задержка;
- действия сил охраны:

— развёртывание,

— пресечение противоправного действия.

Обнаружение определяется как раскрытие действий, совершаемых нарушителями. К функции обнаружения относится оповещение с помощью технических средств о тайных или явных действиях нарушителей.

Система оценки тревожной ситуации должна предоставить силам охраны два вида информации:

- является ли переданный сигнал тревоги истинным или ложным;
- определить место нарушения и численность нарушителей.

Выполнение функции задержки состоит в замедлении продвижения нарушителей по объекту. Задержка может быть обеспечена пассивными (заграждения, замки) и активными (дымогенераторы, строб-вспышки) средствами. Эффективность выполнения функции задержки измеряется длительностью времени, необходимого нарушителям (после их обнаружения) для преодоления каждого из элементов задержки. Задержка нарушителей до их обнаружения не повышает эффективности СФЗ, так как она не предоставляет охране дополнительного времени на развёртывание своих сил и перехват.

Ответные действия сил охраны включают в себя перехват и нейтрализацию нарушителей. Перехват определяется как прибытие сил охраны на тот участок территории объекта, где они могут остановить продвижение нарушителей. Нейтрализация есть сочетание действий, останавливающих нарушителей, перед тем, как они выполнят свою задачу. Эффективность выполнения функций сил охраны определяется временем развёртывания сил охраны, вероятностью развёртывания сил охраны на пути нарушителей и вероятностью успешного исхода столкновения сил охраны с нарушителями [6].

Таким образом, СФЗ должна выполнять функции обнаружения, задержки и ответного действия. Эти функции должны быть выполнены на протяжении интервала времени, меньшего, чем продолжительность времени, необходимого нарушителям для выполнения их задачи (рис. 1).

ПОСТАНОВКА ЗАДАЧИ МОДЕЛИРОВАНИЯ СФЗ

В качестве основных показателей, определяющих опасность реализации угроз и эффективность средств защиты, ниже предлагается выделить временные характеристики этих действий. Будем полагать, что основными требованиями к защищенности информационных ресурсов в объекте являются конфиденциальность, целостность и доступность этих ресурсов [7]. Таким образом, можно выделить множество $R = \{r_i\}$ — множество требований к защищенности информационных

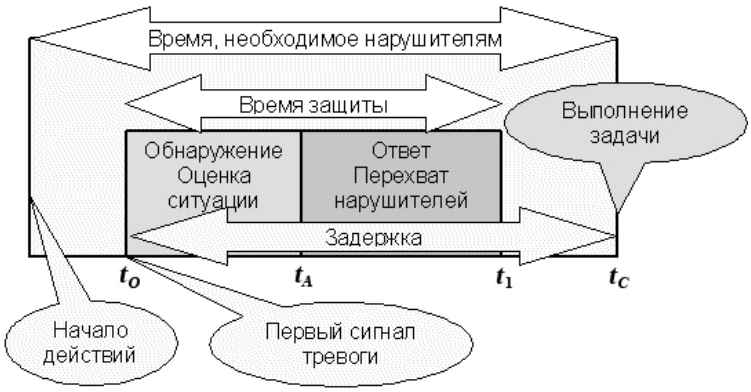

Рис. 1. Зависимость времени выполнения задачи нарушителей от требований к СФЗ

ресурсов. Соответственно, целью реализации угроз (злоумышленных действий) может являться нарушение конфиденциальности, целостности или доступности защищаемых ресурсов, т. е. множество целей злоумышленника представляет собой

$$H = \{h_k\} \subset M \times R,$$

где множество $M = \{m_j\}$ — множество защищаемых информационных ресурсов.

Множество H представляет собой множество всех негативных состояний рассматриваемой информационной системы. Каждому негативному состоянию h_k соответствуют потери (ущерб) C_k от попадания объекта защиты (информационной системы) в данное состояние, которые включают в себя:

- стоимость восстановления данных и работоспособности системы;
- убытки в результате ущерба репутации или разглашения конфиденциальной информации;
- убытки в результате простоя производства во время восстановления ресурса.

Для того чтобы перевести систему в негативное состояние h_k, злоумышленнику необходимо выполнить упорядоченную последовательность действий, связанных с изменением состояний системы $D^k = \{d_0, d_1^k, ..., d_n^k, h_k\}$, где d_0 — работоспособное состояние системы при отсутствии атак на нее, причем не обязательно, чтобы $D^i \cap D^j = \emptyset (i \neq j, i = 1, 2, ..., N-1, j = 1, 2, ..., N$, где N — число негативных состояний).

Часть состояний (или все) $d_1^k, ..., d_n^k$ являются также работоспособными состояниями системы.

Рассмотренный выше набор действий D^k можно также представить в виде цепи, описывающей последовательное изменение состояний системы в процессе совершения злоумышленником атаки h_k.

Граф $A = D^1 \cup D^2 \cup ... \cup D^N$ есть граф, описывающий все возможные изменения состояния защищаемой системы в процессе любой из атак h_k при условии, что никакие две атаки не могут быть проведены одновременно.

Аналогично может быть составлен граф A^* реакции системы защиты на атаки, который показывает изменение состояния информационной системы в процессе восстановления после атаки или в случае обнаружения действий злоумышленника. При этом множество его вершин $V^* = H \cup A^1 \cup A^2 \cup A^3$, где $A^1 = \{a_{k_1}^1\}$ — множество состояний, в которые переходит система в результате восстановления после атаки, $A^2 = \{a_{k_2}^2\}$ — множество действий злоумышленника, которые может обнаружить система защиты, $A^3 = \{a_{k_3}^3\}$ — множество состояний, в которые переходит информационная система в результате реакции системы защиты на действия злоумышленника.

Граф $A^0 = A \cup A^*$ описывает изменения состояния информационной системы в результате действий злоумышленника и действий системы защиты.

Преобразуя матрицу смежности графа A^0 в матрицу переходных вероятностей, соответствующих вероятностям изменения состояния информационной системы, получим ее стохастическую сетевую модель (марковскую модель) в дискретном времени. Для этого единичные элементы матрицы смежности заменяются переходными вероятностями, равными $p_{ij} = \lambda_{ij} \Delta t$, где Δt соответствует периоду времени, в течение которого может быть совершено не более одного перехода при наличии данного барьера; $\lambda_{i,j}$ — интенсивность события преодоления совокупности защитных барьеров злоумышленником при переходе из i-го в j-е состояние или интенсивность

действий системы защиты при ее реагировании на действия злоумышленника, или интенсивность восстановления системы в случае перехода ее в одно из негативных состояний.

На практике величина Δt определяется исходя из выражения $\Delta t = 1 \Big/ \sum_i \lambda_i$, где $\sum_i \lambda_i$ — сумма интенсивностей всех переходов в системе. Величина λ_i в случае экспоненциального закона распределения вероятности реализации i-го события в системе определяется исходя из соотношения $\lambda_i = 1/t_i$, где t_i — среднее время, необходимое для выполнения i-го действия в системе, которое зависит от:

- прочности защитных преград, которые необходимо преодолеть злоумышленнику;
- времени, необходимого для того чтобы обнаружить факт нарушения безопасности;
- времени реакции средств защиты на обнаруженную атаку;
- времени восстановления системы после атаки.

В общем случае сценарий развития атаки представлен на рис. 2.

Общее время реализации атаки $T_{\text{атаки}} = t_{\text{a1}} + t_{\text{a2}} + t_{\text{a3}} + t_{\text{a4}}$ есть случайная величина, где t_{a1}, t_{a2}, t_{a3}, t_{a4} — случайные величины. Сценарий реакции на атаку приведен на рис. 3.

Здесь $t_{\text{защ1}}$, $t_{\text{защ2}}$, $t_{\text{защ3}}$ — также случайные величины. Различные комбинации случайных величин t_{a1}, t_{a2}, t_{a3}, t_{a4} и $t_{\text{защ1}}$, $t_{\text{защ2}}$, $t_{\text{защ3}}$ порождают различные варианты развития атаки.

Таким образом, аналитику, составляющему модель защищенной системы, для каждого негативного состояния из множества H необходимо сопоставить все возможные пути реализации соответствующей атаки, необходимые подготовительные действия, а также все возможные реакции системы защиты на развитие атаки и ее подготовку.

Вероятность нахождения информационной системы в j-м состоянии после n интервалов времени рассчитывают по формуле

$$P_j(n) = M_0 \cdot P^n \cdot D_j, \qquad (1)$$

где $M_0 = [P_1(0)\ P_2(0)\ ...\ P_N(0)]_{1\times N}$ — вектор-строка вероятностей начального состояния системы; $P = [p_{ij}]_{N\times N}$ — квадратная матрица переходных вероятностей; $D_j = [0\ 0\ ...\ 1\ ...\ 0]^T_{N\times 1}$ — вектор-столбец индикатора анализируемого состояния, который имеет все нулевые элементы и одну единицу, которая стоит в позиции, соответствующей порядковому номеру анализируемого состояния [8, 9]. Финальные вероятности нахождения системы в j-м состоянии рассчитываются при условии $n \to \infty$.

На основе рассчитанных таким образом финальных вероятностей рассчитываются среднеожидаемые потери в объекте от действия угроз

$$C_\Sigma = \sum_k P_k C_k, \qquad (2)$$

где P_k — финальная вероятность нахождения системы в состоянии h_k, C_k — ущерб от попадания защищаемой системы в данное состояние.

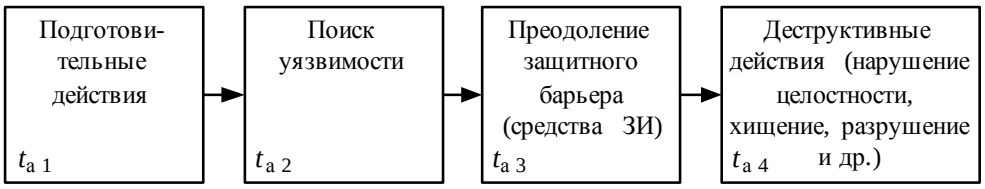

Рис. 2. Сценарий развития атаки

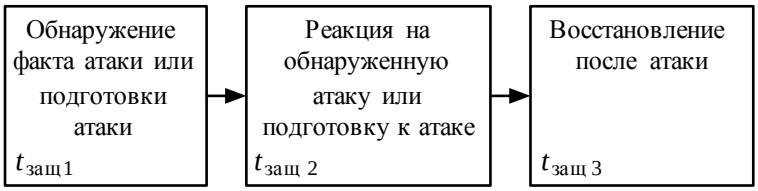

Рис. 3. Сценарий реакции на атаку

ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ МОДЕЛИРОВАНИЯ СФЗ

Для целей моделирования СФЗ авторами был написан программный продукт оценки рисков на основе марковских сетевых моделей [10]. Схема программного продукта приведена на рис. 4.

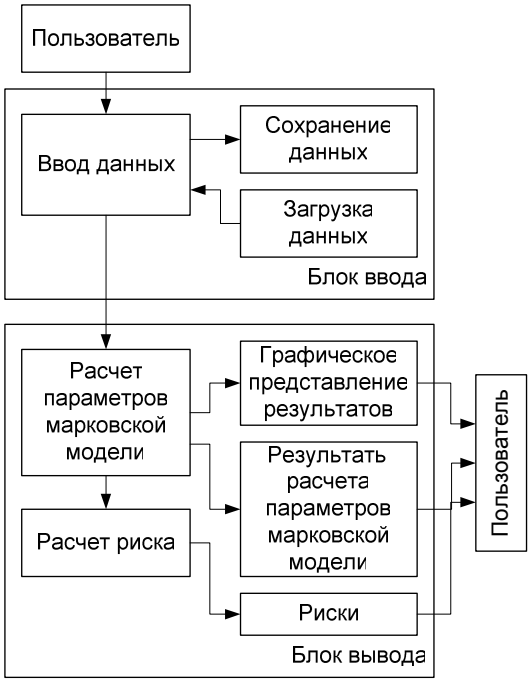

Рис. 4. Схема программного продукта

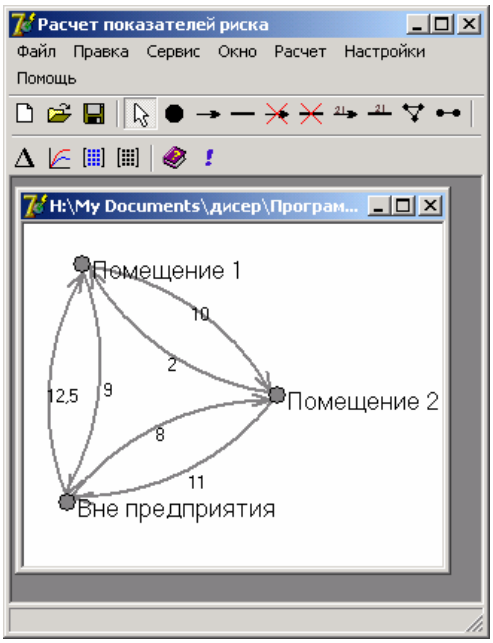

Рис. 5. Пример построения графовой модели

СТРУКТУРА ИСХОДНЫХ ДАННЫХ

Исходные данные о системе защиты вводятся пользователем в виде графовой модели, которая строится им на основании информации о структуре защищаемых ресурсов, средств защиты, и учитывает возможные угрозы для объекта защиты, существующие уязвимости и сценарии развития атак (рис. 5).

На основе вводимых пользователем исходных данных о времени задержки злоумышленника барьерами и времени реакции сил защиты в программном продукте, рассчитываются финальные вероятности доступа к защищаемым ресурсам, на основе которых, в свою очередь, рассчитывается риск, возникающий в связи с реализацией атаки.

ВЫХОДНЫЕ ДАННЫЕ

Как видно из рис. 4, программный продукт предоставляет пользователю три основных группы результатов: графики финальных вероятностей P_k наступления различных исходов в зависимости от времени, прошедшего от начала атаки (рис. 6), значения финальных вероятностей P_k, а также среднеожидаемый ущерб (риск) C_k и C_Σ от попадания системы в рассматриваемые состояния (рис. 7).

ПРИМЕР МОДЕЛИРОВАНИЯ СФЗ

В качестве примера рассмотрим административное здание, план которого приведен на рис. 8. Желтыми маркерами обозначены номера помещений, которые также соответствуют номерам состояний $A = \{A_1, A_2, ...A_n\}$, в которые попадает злоумышленник в процессе реализации атаки. В качестве основных барьерных элементов рассматриваются окна (время взлома Т1а, Т1б, ... ,Т20а) и двери (время взлома $\tau 1, \ldots, \tau 22$). Показателем эффективности действий охраны служит время прибытия охраны ($t1, \ldots, t20$).

Граф путей доступа злоумышленника в охраняемые помещения показан на рис. 9. На основе графа путей доступа строится марковская модель.

Исходные данные для расчета, полученные экспертным путем, приведены в табл. 1–3. При определении значений использовались такие сопутствующие факторы как: высота окон над землей, наличие близкорасположенных построек, укрепленность дверей, а также возможность скрытного приближения к рассматриваемому участку внешнего периметра здания.

Результаты расчета приведены в табл. 4.

Таким образом, суммарный риск составляет 37 058 рублей.

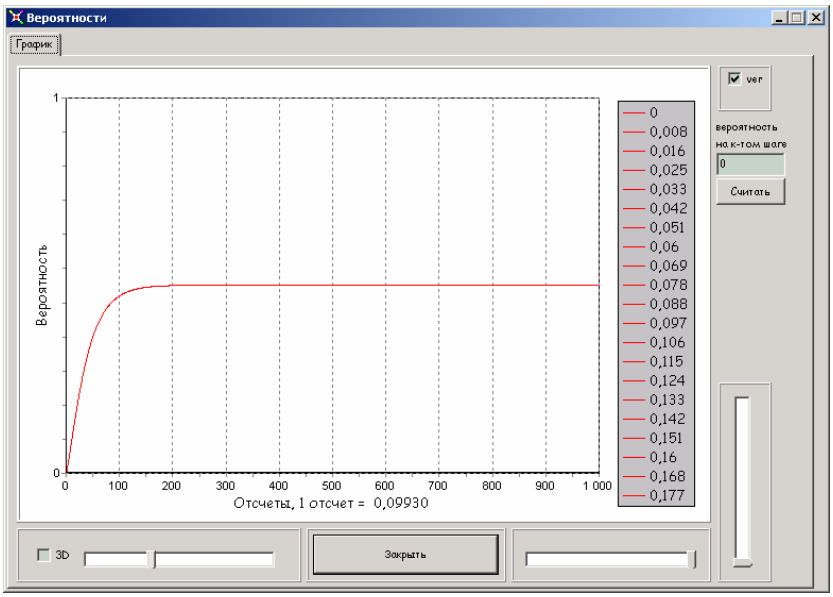

Рис. 6. График изменения финальной вероятности доступа в помещение № 1

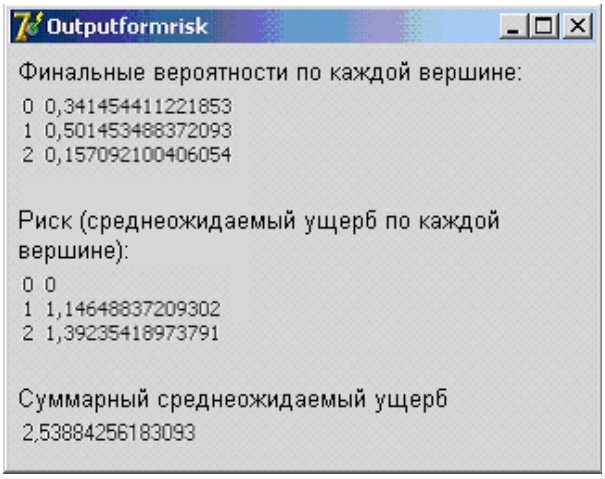

Рис. 7. Результаты работы программы моделирования

Таблица 1

Характеристики барьерных элементов (окна)

№ окна	значение	№ окна	значение	№ окна	значение	№ окна	значение
1a	5	6a	20	11a	10	16a	5
1b	7	6b	19	11b	9	16b	6
2a	14	7a	13	12a	3	17a	20
2b	10	7b	14	12b	4	17b	19
3a	10	8a	8	13a	17	18a	18
3b	11	8b	9	13b	15	18b	19
4a	4	9a	16	14a	9	19a	12
4b	6	9b	16	14b	10	19b	10
5a	18	10a	14	15a	11	20a	10
5b	18	10b	14	15b	15	20b	12

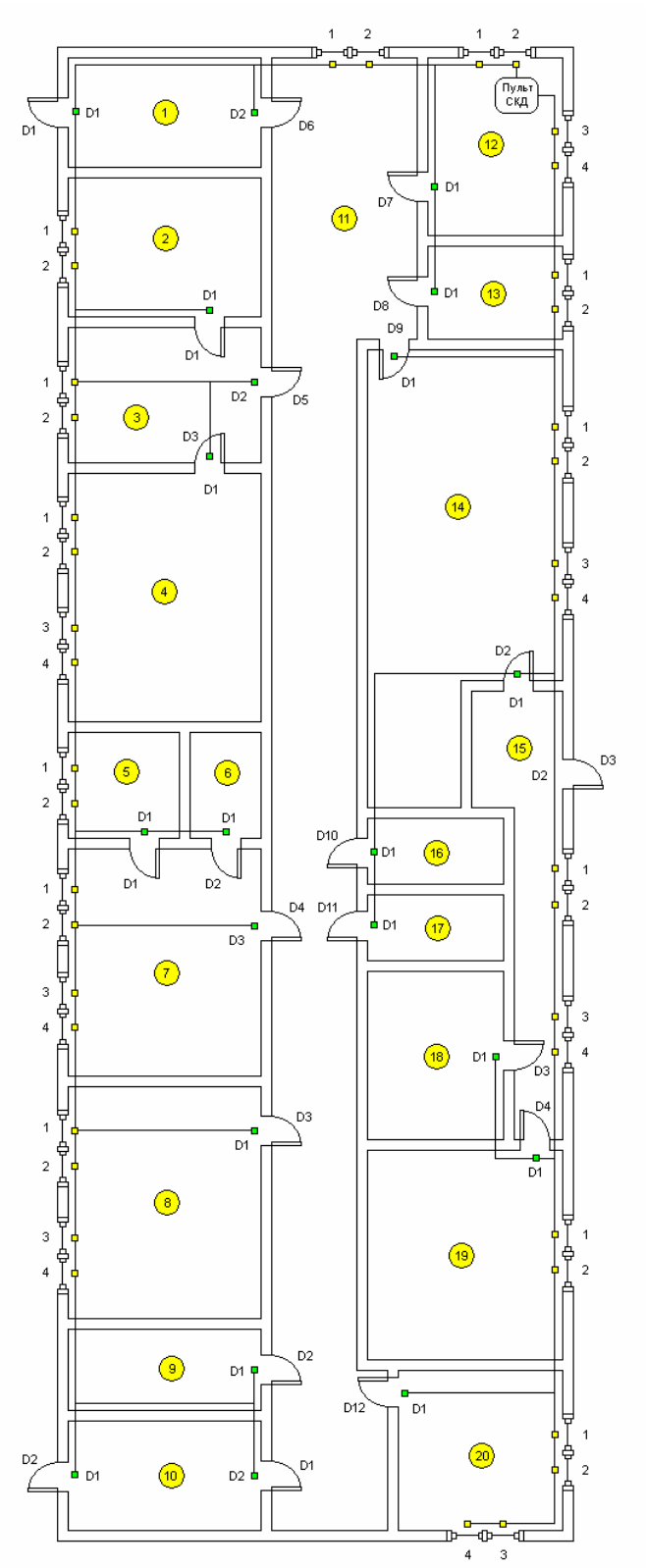

Рис. 8. План административного здания

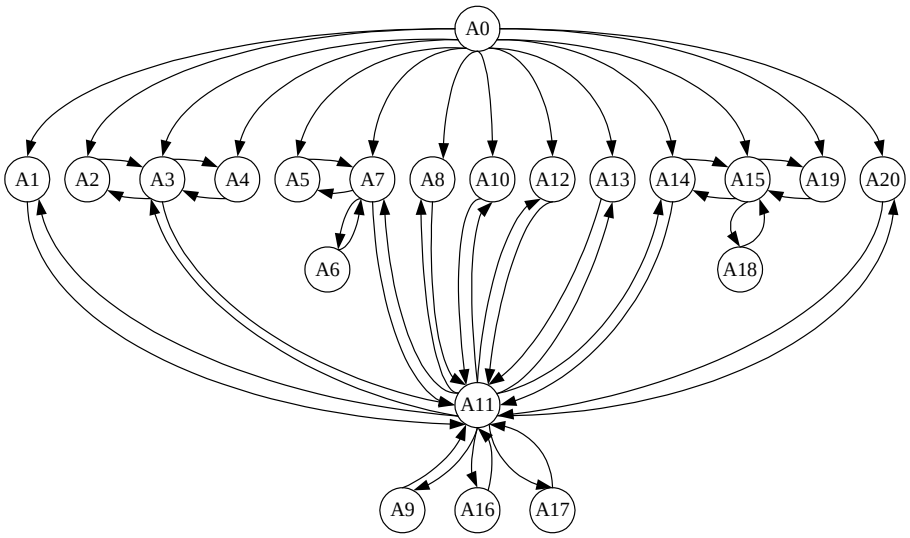

Рис. 9. Граф путей доступа злоумышленника в охраняемые помещения

Таблица 2

Характеристики барьерных элементов (двери)

№ двери	значение	№ двери	значение	№ двери	значение	№ двери	значение
1	15	7	12	13	17	19	30
2	20	8	12	14	13	20	12
3	19	9	20	15	12	21	10
4	9	10	11	16	8	22	15
5	13	11	28	17	8		
6	25	12	10	18	22		

Таблица 3

Характеристики охраняемых помещений (время прибытия охраны (мин) и стоимость защищаемых ресурсов (руб))

№ помещения	время	стоимость	№ помещения	время	стоимость	№ помещения	время	стоимость
1	7	35000	8	2	256000	15	6	30000
2	3	45500	9	10	26000	16	7	0
3	8	23000	10	13	70000	17	9	0
№ помещения	время	стоимость	№ помещения	время	стоимость	№ помещения	время	стоимость
4	5	34500	11	8	0	18	14	20000
5	12	23000	12	12	32000	19	10	36000
6	13	11500	13	15	65500	20	9	10000
7	9	100000	14	3	33000			

Таблица 4

Результаты расчета

№ помещения	Фин. вероятность	Риск	№ помещения	Фин. вероятность	Риск	№ помещения	Фин. вероятность	Риск
1	0,04314	1510	8	0,01958	5013	15	0,07448	2234
2	0,05128	2333	9	0,00391	102	16	0,00518	0
3	0,05914	1360	10	0,03913	2739	17	0,00533	0
4	0,06976	2406	11	0,04764	0	18	0,00570	114
5	0,04708	1083	12	0,05894	1886	19	0,18016	6486
6	0,00345	39	13	0,04952	3243	20	0,06136	613
7	0,04521	4521	14	0,04152	1370	вне	0,08838	0

ЗАКЛЮЧЕНИЕ

Таким образом, рассмотренный программный продукт позволяет производить оценку риска от воздействия угроз информационной безопасности в защищенной информационной системе. В дальнейшем планируется расширить выполняемые программным продуктом функции и включить в его состав блок принятия решений по оптимизации системы защиты, позволяющий произвести построение системы защиты с оптимальной структурой.

СПИСОК ЛИТЕРАТУРЫ

1. **Мельников, В. В.** Защита информации в компьютерных системах / В. В. Мельников. М. : Финансы и статистика, 1997. 340 с.
2. **Барсуков, В.** Физическая защита информационных систем [Электронный ресурс] / В. Барсуков (http://www.jetinfo.ru/1997/1/1/article1.1.1997.html).
3. **Светогоров, Е. Д.** Система физической защиты ядерных материалов и ядерноопасных объектов. Вводный курс [Электронный ресурс] / Е. Д. Светогоров. 2005. (http://culture.mpca.ru).
4. **Alvisnet.** Концепция безопасности и принципы создания систем физической защиты важных объектов [Электронный ресурс]. (www.alvisnet.ru).
5. **Connect.** Технические основы охраны фирмы // Мир связи. Connect. 2001. № 4–5.
6. **Никитин, А. В.** Телевидение в системах физической защиты : учеб.-метод. пособие [Электронный ресурс] / А. В. Никитин, А. К. Цицулин. (http://www.securitybridge.com/articles/80/11516/).
7. **Зегжда, Д. П.** Как построить защищенную информационную систему / Д. П. Зегжда. СПб. : НПО «Мир и семья–95», 1997. 350 с.
8. **Смирнов, Н. В.** Курс теории вероятности и математической статистики (для технических приложений) / Н. В. Смирнов, Н. В. Дунин-Барковский. М. : Наука, 1969. 500 с.
9. **Васильев, В. И.** Моделирование поведения злоумышленника с целью оценки безопасности объектов информатизации / В. И. Васильев, Т. О. Бабкова // Проблемы управления и моделирования в сложных системах : матер. IV Междунар. конф. Самара, 2002. С. 354–360.
10. **Вишнякова, Т. О.** Программный продукт для расчета показателей риска на основе марковской сетевой модели / Т. О. Вишнякова, В. И. Васильев, В. М. Асадуллин // Принятие решений в условиях неопределенности : межвуз. науч. сб. Уфа, 2005. С. 112–120.

ОБ АВТОРАХ

Вишнякова Татьяна Олеговна, асп. каф. выч. техн. и защ. инф. Дипл. инж. по орг. и технол. защиты информации (УГАТУ, 2001). Готовит дис. в обл. анализа систем физ. защиты.

Васильев Владимир Иванович, проф., зав. каф. выч. техн. и защ. инф. Дипл. инж. по промэлектронике (УГАТУ, 1970). Д-р техн. наук по сист. анализу и автом. управлению (ЦИАМ, 1990). Иссл. в обл. многосвязн., многофункц. и интел. систем.