УДК 004.413.4

Т.В. Лебедева[1]

МЕТОДЫ ПОСТРОЕНИЯ МОДЕЛИ ЗЛОУМЫШЛЕННИКА В КОРПОРАЦИИ

В представленной работе рассматриваются различные методы построения модели злоумышленника, а также оценки необходимых ему ресурсов. Целью нарушителя являются конфиденциальные данные корпорации. К вышеописанным процессам были применены следующие математические методы: линейная теория алгоритмов, теория марковских процессов и др.

Ключевые слова: *математическая модель, конфиденциальная информация, модель злоумышленника, информационная безопасность, уровень защиты.*

T.V. Lebedeva

METHODS OF CONSTRUCTING A MODEL OF INTRUDER IN CORPORATION

In the article the different methods of constructing of the model intruder, and estimates of the resources it requires are presented. The purpose of the offender is confidential corporate data. By the above processes mathematical methods include: linear algorithm theory, the theory of Markov processes and others methods had been applied.

Keywords: *mathematical model, confidential information intruder model, information security, level of protection.*

Процесс безопасного хранения конфиденциальных данных является одной из приоритетных задач службы безопасности компании. Для решения поставленной задачи необходимо провести исследование не только среды, процесса хранения информации и выявление слабых мест в защите данных, но и провести исследование компании, направленное на обнаружение потенциальных злоумышленников.

На данный момент эксперты в сфере информационной безопасности выделяют две категории злоумышленников: внешние и внутренние. К первой категории относят нарушителей, которые не имеют непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны. Ко второй относят нарушителей, которые имеют непосредственный доступ к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Построение модели нарушителя – достаточно трудоемкий процесс. Рассмотрим несколько подходов к решению данной задачи.

Формальная модель нарушителя информационной безопасности

Согласно «Методическим рекомендациям органам исполнительной власти города Москвы по организации защиты конфиденциальной информации и персональных данных» [1], формальная модель вероятного нарушителя должна включать в себя:

– описание возможных нарушителей;

– предположения об имеющейся у нарушителя информации об объектах атак;

– предположения об имеющихся у нарушителя средствах атак;

– описание объектов и целей атак;

– описание каналов атак.

Миронова В.Г. и Шелупанов А.А. в своей работе «Модель нарушителя безопасности конфиденциальной информации» [2] предлагают модель злоумышленника представлять в виде таблицы, тем самым систематизируя данные проведенного анализа полученной в ходе исследования информации (табл. 1).

После систематизации знаний о предполагаемых нарушителях для ИС обработки конфиденциальной информации, разрабатывается модель

[1] Аспирант НОУ ВПО «Российский новый университет».

угроз безопасности информации [2]. Предложенный метод позволяет построить достаточно информативную модель злоумышленника, которая дает представление о возможностях нарушителя, принадлежащего к той или другой группе злоумышленников. Однако же построенная модель не показывает взаимосвязи процесса хищения информации и требуемого времени, необходимого для реализации задуманного правонарушения.

Таблица 1

№ п/п	Подгруппы	Обозначение	Рубеж (зона) защиты	Характеристика нарушителя	Возможности
1.	Первая подгруппа внутренних нарушителей	M_1	Зона 1. Территория объекта, телекоммуникации	Лица, имеющие санкционированный доступ на территорию организации, но не имеющие доступа в здание и помещения, в которых расположена ИС	Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы здания; осуществлять перехват информации по техническим каналам
2.	Вторая подгруппа внутренних нарушителей	M_2	Зона 2. Здание объекта, телекоммуникации	Лица, имеющие санкционированный доступ в здание, но не имеющие доступа в служебные помещения, в которых расположена ИС	Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений; осуществлять перехват информации по техническим каналам; располагать информацией о размещении поста охраны, системе видеонаблюдения и т.д., помещений для приема посетителей
3.	Третья подгруппа внутренних нарушителей	M_3	Зона 3. Представительские помещения, ПЭВМ, коммуникации, помещения для приема посетителей	Лица, имеющие санкционированный доступ в здание только в специально отведенные помещения (помещения для приема посетителей), но не имеющие доступа в служебные помещения, в которых расположена ИС	Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений; осуществлять перехват информации по техническим каналам; располагать информацией о размещении поста охраны, системе видеонаблюдения и т.д., помещений для приема посетителей
4.	Четвертая подгруппа внутренних нарушителей	M_4	Зона 4. Кабинеты пользователей ИС, администраторов ИС	Зарегистрированные пользователи ИС, осуществляющие ограниченный доступ к ресурсам ИС с рабочего места	Иметь доступ к фрагментам конфиденциальной информации; располагать фрагментами информации о топологии ИС (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; располагать именами и вести выявление паролей зарегистрированных пользователей; изменять конфигурацию технических средств ИС, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИС; знать, по меньшей мере, одно легальное имя доступа; обладать всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству конфиденциальной информации; располагать конфиденциальными данными, к которым имеет доступ
5.	Пятая подгруппа внутренних нарушителей	M_5	Зона 5. Серверные, комнаты конфиденциальных переговоров, ПЭВМ, телекоммуникации	Зарегистрированные пользователи сервера ИС с полномочиями администратора безопасности сегмента (фрагмента) ИС	Обладает всеми возможностями M_4; имеет право санкционированного доступа в помещение, в котором установлено серверное оборудование; имеет санкционированное имя пользователя для настройки сегмента (фрагмента) ИС

Линейная теория алгоритмов в решении задачи оценки времени, необходимого злоумышленнику для изучения системы защиты информации

В работе [3] Иванов В.П. предлагает оценивать требуемое время, необходимое для изучения системы защиты информации, с помощью теории алгоритмов. Рассмотрим подробно предлагаемую методику.

Пусть имеется написанная на некотором алгоритмическом языке программа длиной N бит, которая по сложности соизмерима с написанием программы длиной N бит на том же языке. Для определения среднего времени изучения программы (T) воспользуемся аппроксимацией уравнения времени, необходимого для написания программы. Тогда среднее время будет рассчитываться по формуле (1):

$$T = \frac{N^2 \times \log_2 \eta}{4S} \text{ [c]}, \qquad (1)$$

где η – алфавит языка текста программы;

S – число Страуда (S = 4÷20 операций в секунду), характеризующее количество объектов, которыми может оперировать злоумышленник одновременно (своего рода характеристика быстродействия злоумышленника, изучающего текст программы);

N – длина текста программы (команды + операнды) в битах.

Если программа написана на машинном языке, то, согласно методу Холстеда, время будет определено формулой (2)

$$T \approx N \text{ , [c]}. \qquad (2)$$

Поскольку программы защиты информации характеризуются большой длиной, а работа злоумышленника характеризуется утомляемостью, введем поправку на утомляемость злоумышленника. Тогда выражение для T будет описываться формулой (3)

$$T \approx 3N \text{ , [c]}. \qquad (3)$$

Построение модели злоумышленника с использованием марковских процессов

Рассмотрим методику построения модели злоумышленника, предлагаемую Цыбулиным А.М. и Шипилевой А.В. [4], которые предлагают для построения математической модели злоумышленника использовать однородные марковские докритические ветвящиеся процессы.

Пусть случайные величины Z_0, Z_1, Z_2, … – число уязвимостей в нулевом, первом, втором и т.д. уровнях защиты корпоративной сети – соответствуют числу вершин (состояний) корневого ориентированного дерева уязвимостей. Дугам дерева уязвимостей приписаны вероятности перехода из состояния i-го уровня защиты в состояние $(i + 1)$-го уровня. Длительность пребывания в каждом состоянии нулевого, первого, и т.д. уровнях защиты равна, соответственно, T_0, T_1, T_2, … .

Всегда полагается $Z_0 = 1$ с вероятностью 1 и математическое ожидание количества уязвимостей на первом уровне защиты $EZ_1 < 1$. Обозначим через P вероятностную меру процесса. Тогда распределение вероятностей случайной величины Z_1 определяется числами $P\{Z_1 = k\} = p_k$, $k = 0, 1, 2, \ldots$, $\sum p_k = 1$, где p_k интерпретируется как вероятность того, что уязвимость, существующая на первом уровне защиты, обеспечивает доступ к уязвимостям на втором уровне.

Условное распределение Z_{i+1} при условии $Z_i = k$ определяется из предположения, что разные уязвимости порождают другие уязвимости независимо. Отсюда вытекает, что Z_{i+1} распределена как сумма k независимых случайных величин, каждая из которых распределена так же, как Z_1. Если $Z_i = 0$, то с вероятностью 1 $Z_{i+1} = 0$.

Переходные вероятности рассматриваемого марковского процесса задаются в виде:

$$P_{ij}(\tau, t) = P_{ij}\{Z_{n+1}(t) = j \mid Z_n(t) = i\},$$
$$i.j, n = 0, 1, 2, \ldots; 0 \le \tau \le 1. \qquad (6)$$

В процессе исследования модели (6) используются прямое и обратное уравнения Колмогорова и определяются: распределение вероятностей и моменты случайной величины Z_t; вероятность того, что случайная последовательность Z_0, Z_1, Z_2, … сходится к нулю (злоумышленник не может использовать уязвимости для проведения атак); поведение последовательности в случае, когда она не сходится к нулю, т.е. достигнет ли злоумышленник цели.

$$\begin{cases} \dfrac{\partial P_{ik}(\tau, t)}{\partial t} = -kb(t)P_{ik}(\tau, t) + b(t)\sum\limits_{j=1}^{k+1} P_{ik}(\tau, t)\, jp_{k-j+1}(t), \\ P_{ik}(\tau, \tau + 0) = \delta_{ik}. \end{cases} \qquad (7)$$

Здесь $\delta_{ik} = 1$ при $i = k$, а $\delta_{ik} = 0$ при $i \ne k$.

$$\begin{cases} \dfrac{\partial P_{ik}(\tau, t)}{\partial \tau} = ib(\tau)P_{ik}(\tau, t) - ib(\tau)\sum\limits_{j=i-1}^{\infty} P_{jk}(\tau, t)\, p_{j-i+1}(\tau),\ i > 0 \\ \dfrac{\partial P_{0k}(\tau, t)}{\partial \tau} = 0, P_{ik}(t - 0, t) = \delta_{ik}, \end{cases} \qquad (8)$$

где $b(t)\Delta + o(\Delta)$ – вероятность, что уязвимость, которая в момент времени t используется злоумышленником для своей атаки, к моменту времени $(t + \Delta)$ завершится успехом. Если уязвимость используется в момент τ, то с вероятностями $p_1(\tau), p_2(\tau), p_3(\tau), \ldots$ злоумышленнику

становятся доступны 1, 2, 3, … новых уязвимостей. В соответствии с «Теорией ветвящихся случайных процессов» Т. Харриса [6] определяются величины $b_i(t) = ib(t)$ и $p_{ij}(t) = p_{j-i+1}(t)$. Часто вместо переходных вероятностей однородного ветвящегося процесса используются соответствующие производящие функции [5].

Предлагаемая модель злоумышленника

В работах [7]–[17] нами рассматривалась оценка рисков потери конфиденциальной информации с разных точек зрения, однако не затрагивалась модель злоумышленника с точки зрения влияния уровня натиска (с целью нарушить систему безопасности организации) на уровень защиты конфиденциальных данных компании.

Рассмотрим ситуацию, когда при повышении уровня натиска на систему безопасности уровень защиты конфиденциальных данных корпораций остается неизменным. Такая ситуация возможна в случае, если служба безопасности утвердила наижесточайшую политику, не соизмеримую с возможными попытками взломов системы защиты.

Предположим, что зависимость уровня защиты конфиденциальных данных от уровня натиска злоумышленника определяется по формуле (9).

$$y(x) = 5. \quad (9)$$

В таблице 2 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

Таблица 2

№ п/п	Уровень натиска, x	Уровень защиты, $y(x)$
1	0	5
2	1	5
3	2	5
4	3	5
5	4	5
6	5	5
7	6	5
8	7	5
9	8	5
10	9	5
11	10	5

На основании данных, указанных в табл. 2, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 1). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд.

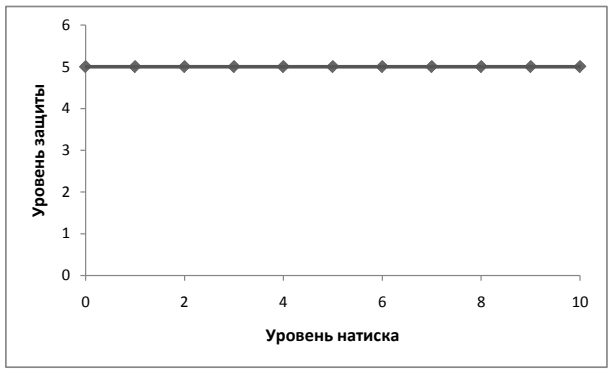

Рис. 1. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Уровень защиты постоянен

Взаимоотношение уровня защиты к уровню натиска, проиллюстрированное рис. 1, является ярким примером ситуации, когда уровень защиты конфиденциальных данных превосходит уровень возможного натиска с целью преодоления барьеров защиты.

Рассмотрим ситуацию, когда при повышении уровня натиска на систему безопасности политика безопасности ужесточается. Такая ситуация возможна в случае, если служба безопасности проводит регулярный мониторинг на наличие угроз и атак и в случае их обнаружения оперативно реагирует на их наличие, ужесточая политику.

Предположим, что зависимость уровня защиты конфиденциальных данных от уровня натиска злоумышленника определяется по формуле (10).

$$y(x) = x + 3. \quad (10)$$

В таблице 3 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

Таблица 3

№ п/п	Уровень натиска, x	Уровень защиты, $y(x)$
1	0	3
2	1	4
3	2	5
4	3	6
5	4	7
6	5	8
7	6	9
8	7	10
9	8	11
10	9	12
11	10	13

На основании данных, указанных в табл. 3, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 2). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд.

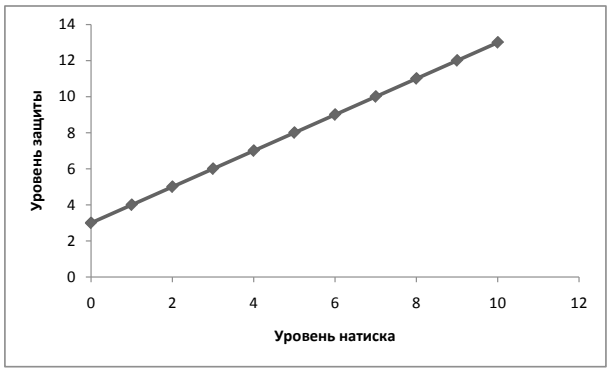

Рис. 2. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Уровень защиты пропорционален уровню натиска

Взаимоотношение уровня защиты к уровню натиска, проиллюстрированное рис. 2, является ярким примером ситуации, когда меры безопасности соизмеримы с мерами, применяемыми к ее нарушению.

Следующая ситуация, которую мы предлагаем рассмотреть читателю, – это ситуация, когда при повышении уровня натиска на систему безопасности уровень защиты падает. Такая ситуация возможна в случае, если служба безопасности не проводит регулярного мониторинга на наличие угроз и атак, либо в случае утери конфиденциальной информации компании будет принесен ущерб, не превышающий стоимости обеспечения сохранности данных.

Предположим, что зависимость уровня защиты конфиденциальных данных от уровня натиска злоумышленника определяется по формуле (11).

$$y(x) = \begin{cases} 18, & x < 2 \\ -2x + 22, & x \geq 2 \end{cases}. \qquad (11)$$

В табл. 4 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

На основании данных, указанных в табл. 4, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 3). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд.

Таблица 4

№ п/п	Уровень натиска, x	Уровень защиты, $y(x)$
1	0	18
2	1	18
3	2	18
4	3	16
5	4	14
6	5	12
7	6	10
8	7	8
9	8	6
10	9	4
11	10	2

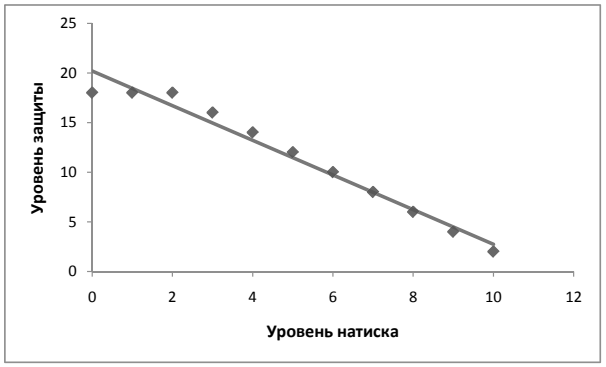

Рис. 3. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Уровень защиты обратно пропорционален уровню натиска

На рис. 3 проиллюстрирована ситуация, когда уровень защиты конфиденциальных данных снижается под натиском злоумышленника.

Рассмотрим ситуацию, когда при повышении активности злоумышленника уровень защиты конфиденциальных данных корпораций повышается, но в конкретный момент времени система безопасности не выдерживает натиска, и закрытая информация становится доступной. Данная ситуация является одним из примеров проявления теории катастроф.

Предположим, что зависимость уровня защиты конфиденциальных данных от уровня натиска злоумышленника определяется по формуле (12).

$$y(x) = -x^2 + 10x. \qquad (12)$$

В табл. 5 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

Таблица 5

№ п/п	Уровень натиска, *x*	Уровень защиты, *y*(*x*)
1	0	0
2	1	9
3	2	16
4	3	21
5	4	24
6	5	25
7	6	24
8	7	21
9	8	16
10	9	9
11	10	0

На основании данных, указанных в табл. 5, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 4). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд.

Рис. 4. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Уровень защиты изменяется по параболе

Одним из примеров, проиллюстрированным рис. 4, является ситуации, когда со временем увеличивается квалификация злоумышленника и, как следствие, – уровень натиска, под которым система безопасности перестает функционировать.

Рассмотрим ситуацию, когда при повышении уровня натиска на систему безопасности политика безопасности ужесточается, но в один из моментов натиск злоумышленника приводит к тому, что уровень защиты падает, в результате чего доступ к конфиденциальной информации становится открытым злоумышленнику, но служба безопасности, обнаружив утечку, проводит мероприятия по ее устранению, в связи с чем уровень защиты увеличивается.

Предположим, что зависимость уровня защиты конфиденциальных данных от уровня натиска злоумышленника определяется по формуле (13).

$$y(x) = 1 + \sin(x). \qquad (13)$$

В табл. 6 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

Таблица 6

№ п/п	Уровень натиска, *x*	Уровень защиты, *y*(*x*)
1	1	0
2	1,282	0,286
3	1,541	0,571
4	1,756	0,857
5	1,910	1,142
6	1,990	1,428
7	1,990	1,714
8	1,910	1,999
9	1,756	2,285
10	1,541	2,570
11	1,282	2,856
12	1	3,142
13	0,718	3,427
14	0,459	3,713
15	0,244	3,998
16	0,090	4,284
17	0,010	4,570
18	0,010	4,855
19	0,090	5,141
20	0,244	5,426
21	0,459	5,712
22	0,718	5,998
23	1	6,283

На основании данных, указанных в табл. 6, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 5). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд.

Стоит заметить, что на данном графике проиллюстрированы два примера проявления теории катастроф, как с точки зрения компании, так и с точки зрения злоумышленника.

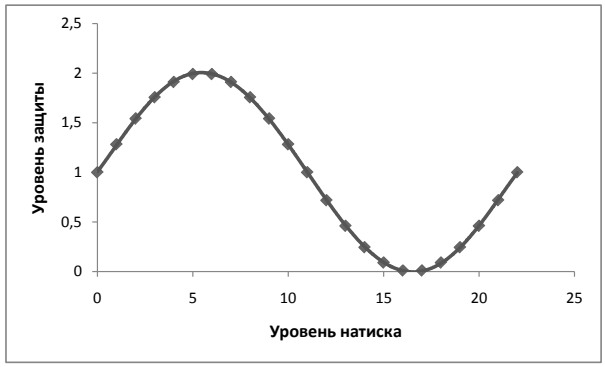

Рис. 5. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Уровень защиты изменяется циклически

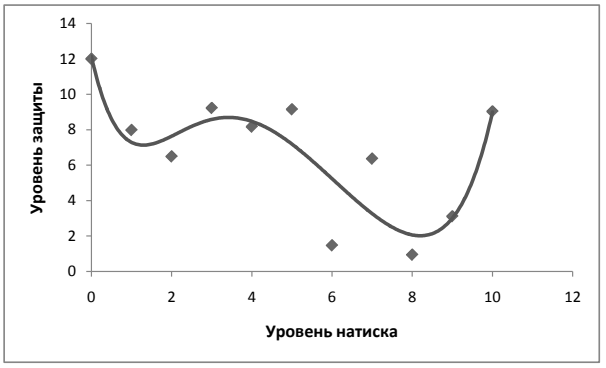

Рис. 6. Взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника. Взаимосвязи нет

Рассмотрим ситуацию, когда в компании нет конкретной политики безопасности. В этом случае все мероприятия направлены не на предупреждение утечки конфиденциальной информации, а на устранение их последствий. В табл. 7 представлены оценки уровня защиты и уровень натиска в зависимости от времени.

Таблица 7

№ п/п	Уровень натиска, x	Уровень защиты, $y(x)$
1	0	12
2	1	7,975
3	2	6,485
4	3	9,222
5	4	8,167
6	5	9,146
7	6	1,463
8	7	6,360
9	8	0,935
10	9	3,105
11	10	9,030

На основании данных, указанных в табл. 7, построим график функции, описывающей взаимосвязь между уровнем защиты конфиденциальной информации компании и уровнем натиска злоумышленника (рис. 6). На рисунке точками обозначен график функции взаимосвязи, линией – его тренд, уравнение которого определяется по формуле (14).

$$y(x) = 0{,}0006x^6 - 0{,}0212x^5 + 0{,}2926x^4 - $$
$$- 2{,}0497x^3 + 6{,}9974x^2 - 10{,}07x + 12{,}14. \quad (14)$$

Также рисунок 6 описывает ситуации, когда ни со стороны компании, ни со стороны злоумышленника нет конкретного плана работ и все действия выполняются случайно.

Заключение

Таким образом, в настоящей работе нами были рассмотрены различные подходы к исследованию модели злоумышленника как с использованием формального подхода, так и с использованием математического аппарата.

Использование предложенных методов позволяет экспертам получить всестороннюю модель потенциального злоумышленника, что является одним из главных критериев, применяемых при оценке рисков потери конфиденциальной информации.

Литература

1. Методические рекомендации органам исполнительной власти города Москвы по организации защиты конфиденциальной информации и персональных данных. – Департамент информационных технологий города Москвы, 2010 г.

2. Миронова В.Г., Шелупанов А.А. Модель нарушителя безопасности конфиденциальной информации // Информационная безопасность систем. – 2012. – № 1(31).

3. Иванов В.П. Математическая оценка защищенности информации от несанкционированного доступа // Специальная техника. – 2004. – № 1.

4. Матвеев В.Ф. и др. Системы массового обслуживания. – М. : Изд-во Московского университета, 1984.

5. Цыбулин А.М., Шипилева А.В. Математическая модель злоумышленника в корпоративной сети // Управление большими системами. – 2007. – Выпуск 19.

6. Харрис Т. Теория ветвящихся случайных процессов. – М. : Мир, 1966. – 355 с.

7. Крюковский А.С., Лебедева Т.В. Оценка информационных рисков и экспертный ана-

лиз // Сборник научных трудов по материалам международной научно-практической конференции «Современные направления теоретических и прикладных исследований, 2011». – Одесса, 2011. – Т. 3. – С. 18–21.

8. Лебедева Т.В. Риски: оценка и управление информационными рисками // Вестник Российского нового университета. Серия «Управление, вычислительная техника и информатика». – М. : РосНОУ, 2010. – Вып. 3. – С. 64–66.

9. Лебедева Т.В. Автоматизированные средства анализа и управления информационными рисками // Сборник материалов VI Международной научно-исследовательской конференции «Наука и современность – 2010». – Новосибирск : ЦРНС, 2010. – С. 116–120.

10. Крюковский А.С., Лебедева Т.В. Разработка автоматизированной системы статистического анализа рекламной деятельности // Труды X Международной научной конференции «Цивилизация знаний: проблемы модернизации России», г. Москва, 24–25 апреля 2009 г. – М. : РосНОУ, 2009. – С. 339–343.

11. Крюковский А.С., Лебедева Т.В. Методики оценки стоимости конфиденциальной информации и экспертный анализ // Материалы Всероссийской конференции студентов и молодых ученых с международным участием «Молодежная наука в развитии регионов». – Пермь : Березниковский филиал ПГТУ, 2011. – С. 38–41.

12. Крюковский А.С., Лебедева Т.В. Методика оценки рисков утери конфиденциальной информации в компании // Вестник Российского нового университета. Серия «Управление, вычислительная техника и информатика». – М. : РосНОУ, 2011. – Вып. 4. – С. 55–63.

13. Крюковский А.С., Лебедева Т.В., Скородумов Б.И. Программно-аналитический комплекс для экспертных оценок стоимости конфиденциальной информации // Материалы X Международной научно-методической конференции «Информатика: проблемы, методология, технологии», Воронеж, 11–12 февраля 2010 г. – Т. 1. – Воронеж : Издательско-полиграфический центр Воронежского ГУ, 2010. – С. 384–387.

14. Лебедева Т.В., Крюковский А.С. Методика экспертной оценки рисков потери информации корпорации // Труды XII Международной научной конференции «Цивилизация знаний: проблема человека в науке XXI века», Москва, 22–23 апреля 2011 г. – Часть II. – М. : РосНОУ, 2011. – С. 146–148.

15. Крюковский А.С., Лебедева Т.В. Математическая модель процессов хранения, передачи и потери конфиденциальной информации // Вестник Марийского государственного технического университета. Серия «Радиотехнические и инфокоммуникационные системы». – Йошкар-Ола : МарГТУ, 2012. – № 1(14). – С. 25–36.

16. Крюковский А.С., Лебедева Т.В. Математическая модель процессов хранения, передачи и потери конфиденциальной информации: дискретный и непрерывный случаи // T-Comm: Телекоммуникации и транспорт. – 2012. – № 11. – С. 32–39.

17. Крюковский А.С., Лебедева Т.В. Математическое моделирование процесса потери и хранения конфиденциальной информации // Труды XIII Международной научной конференции «Цивилизация знаний: проблемы и перспективы социальных коммуникаций», Москва, 20–21 апреля 2012 г. – Часть 2. – М. : РосНОУ, 2012. – С. 24–29.