РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

А. Ю. Ермакова[1], А. Б. Лось[2]

[1]Российский технологический университет МИРЭА, Москва, Россия
[2]НИУ «Высшая школа экономики», Москва, Россия
E-mail: a.alla1105@yandex.ru, alexloss2011@mail.ru

В статье рассматриваются вопросы применения риск-ориентированного подхода к оценке защищенности информационных систем. Предлагается развитие данного подхода в части введения нового параметра - промежутка времени, в течение которого информационная система может считаться защищенной. С целью разработки методики оценки указанного параметра предлагается процедура построения прогнозных моделей компьютерных инцидентов на основе поиска непрерывных аппроксимирующих функции по данным о предыдущих инцидентах. Для построения указанных функций разработано специализированное программное обеспечение, позволяющее строить их, как в ручном, так и в автоматическом режиме. В статье дается описание методики построения прогнозной модели, приведена блок-схема программы нахождения непрерывных аппроксимирующих функций, дано описание структуры интерфейса, рассмотрены примеры построения прогнозных моделей для ряда угроз информационным системам и примеры вычисления времени их безопасной работы.

RISK-BASED APPROACH TO ASSESSING THE SECURITY OF INFORMATION SYSTEMS

A. Y. Ermakova, A. B. Los

The article deals with the application of a risk-based approach to assessing the security of information systems. The development of this approach is proposed in terms of introducing a new parameter - the period of time during which an information system can be considered protected. In order to develop a methodology for estimating this parameter, a procedure for constructing predictive models of computer incidents based on the search for a continuous approximating function based on actual data about previous incidents is proposed. For the construction of these functions, specialized software has been developed that allows them to be built both manually and automatically. The article describes the methodology for constructing a predictive model, provides a block diagram of the program for finding a continuous approximating function, the structure of the interface, considers examples of constructing predictive models for a number of threats to information systems and examples of calculating the safe operation time of the latter.

Введение

В работе рассматриваются вопросы развития риск-ориентированного подхода к оценке защищенности информационных систем.

Вопросы оценки защищенности информационных систем (далее – ИС) являются важным моментом их функционирования. В условиях, возникновения событий, вызываемых различными факторами, недостаточное внимание к вопросам обеспечения защищенности процессов передачи, хранения и обработки данных может привести к серьезным последствиям, в частности, к значительному ущербу: потере активов, постоянных клиентов, репутации и многому дру-

гому. С другой стороны, избыточные меры в этом вопросе приводят не только к необоснованным расходам на приобретение, установку и эксплуатацию дорогостоящего оборудования, но и к значительным затруднениям в работе вычислительных комплексов.

В традиционном риск-ориентированном подходе к проблеме оценки уровня защищенности ИС, изложенном, в частности, в отечественных и международных стандартах по ИБ ([1-3]), предполагается вычисление риска *R* нарушения информационной безопасности (далее -ИБ), величина которого находится из соотношения:

$$R = \sum_{i=1}^{n} p(y_i) \cdot u_i, \tag{1}$$

где $p(y_i)$ – вероятность реализации злоумышленником угрозы y_i нарушения ИБ, u_i – величина ущерба от успешного осуществления данной угрозы.

Далее определяется граница допустимых потерь (рисков) R_0 и, в случае выполнения условия

$$R \le R_0$$

информационная система считается защищенной.

В работе [4] предложен, так называемый, временной подход к оценке защищенности ИС, суть которого состоит в определении вида зависимости величин $p(y_i)$ и u_i от времени *t*:

$$p(y_i) = p_{y_i}(t), u_i = u_i(t). \tag{3}$$

В этом случае риск *R* также становится функцией времени *t*:

$$R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t). \tag{4}$$

Поскольку, как правило, величины $p_{y_i}(t)$ и $u_i(t)$ являются неубывающими функциями времени *t*, то уравнение

$$R(t) = \sum_{i=1}^{n} p_{y_i}(t) \cdot u_i(t) = R_0 \tag{5}$$

имеет положительный корень T_0, который можно рассматривать как время безопасной работы ИС, поскольку, через данное время прогнозный риск достигнет максимально допустимого значения и работа системы теоретически перестанет быть безопасной.

Подходы к построению функций $p_{y_i}(t)$, учитывающих вероятность возникновения ущерба, предпринимались ранее в работах [5-7]. В настоящей работе рассматривается методика проведения экспериментальных исследований по построению прогноза возникновения компьютерных инцидентов и вычислению на этой основе величины T_0.

В качестве примера развития подходов к оценке возможных рисков при возникновении компьютерных инцидентов, приводящих к нарушению информационной безопасности, в работе построены прогнозные модели возможного несанкционированного доступа к ресурсам организации и даны рекомендации по вычислению времени безопасной работы информационной системы.

Методика построения прогнозных риск-моделей при инцидентах, приводящих к нарушению информационной безопасности.

Ранее в работах [8-10] рассматривался подход к построению прогнозных моделей интенсивности компьютерных атак и инцидентов, приводящих к нарушению информационной безопасности. Суть данного подхода состоит в построении по известным значениям исследуемых параметров за определенный предшествующий период (узловым точкам) непрерывной «аппроксимирующей» функции $f(x)$, наиболее близко отстоящей от узловых точек (x_i, y_i). Поиск указанной функции осуществляется в виде линейной комбинации элементарных (базовых) функций с применением модернизированного метода наименьших квадратов, суть которого состоит в следующем.

Многочисленные эксперименты показывают, что даже при точном приближении на заданном интервале состояния рассматриваемой динамической системы построенной непрерывной функцией, поведение данной функции вне этого интервала может иметь резкие скачки и, в частности, быстрое возрастание или убывание. Яркий пример невозможности применения для прогнозирования ([9]) выполнен при аппроксимации с помощью полинома Лагранжа, дающего полное совпадение в узловых точках и резко меняющего направление за границами интервала.

Для решения данной проблемы предлагается следующая модификация рассматриваемого метода построения приближающей функции. На первом шаге, как и ранее, осуществляется построение данной функции в виде линейной комбинации базовых функций в ручном или автоматическом режиме. Далее определяется временной интервал, на котором предполагается построение прогнозных значений рассматриваемой динамической системы и вычисляются на нем наибольшее и наименьшее значения построенной функции. В случае выхода их за выбранные границы, определяемые выборочным средним и дисперсией исходных данных, производится замена набора базовых функций. Для построения разработано специальное программное обеспечение, описание которого приведено ниже.

Описание разработанной программы.

Ввод данных. На вход программе подаётся таблично заданная функция. В качестве источника используется файл Excel следующего вида (табл. 1):

В табл. 1 первый столбец A – значения величин x_i, второй столбец B – значения величин y_i. Количество считываемых точек равно количеству использованных строк, поэтому ниже этой таблицы не должно быть занятых ячеек (правее таблицы могут быть не пустые ячейки, они никак не повлияют на работу программы).

Таблица 1

Формат исходных данных

№	A	B
1	1	0, 841471
2	2	0,909297
3	3	0,14112
4	4	- 0,7568
5	5	- 0, 95892
6	6	- 0,27942
7	7	0, 65 698
8	8	0, 989358
9	9	0, 412118
10	10	- 0, 54402
11	11	- 0, 9999
12	12	- 0,53697
13	13	0, 420167
14	14	0, 990607
15	15	0, 650288
16	16	- 0, 2879
17	17	- 0, 9614
18	18	- 0, 75099
19	19	0, 149877
20	20	0,9122945

Интерфейс программы

Интерфейс разработанной программы представлен на рис. 1.

Работа с программой начинается с нажатия кнопки «Чтение таблицы» и выбора файла входных данных. В случае успешного чтения, первая таблица заполняется данными из Excel файла. Если при попытке чтения произошла ошибка, либо файл был пустой, появляется сообщение «Ошибка чтения из файла». После успешного ввода данных становятся доступны остальные функции программы.

Кнопка «МНК 1» запускает алгоритм поиска многочлена аппроксимирующей функцией методом наименьших квадратов с базисными функциями x^i. Степень многочлена можно менять в поле «Степень». При этом в первой таблице в четвёртом столбце $f(x_i)$ появятся значения аппроксимирующей функции в заданных точках, будет построен график и посчитано среднеквадратическое отклонение по узлам таблично заданной функции.

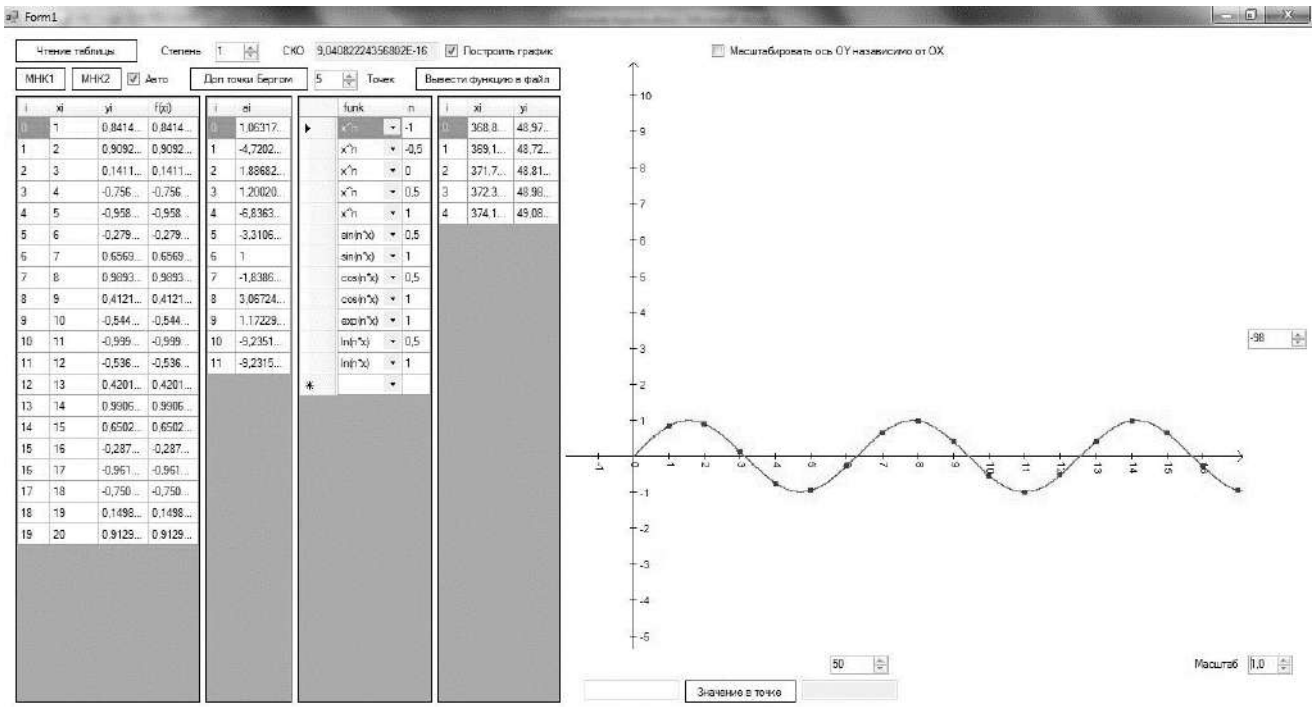

Рис. 1. Интерфейс программы

Коэффициенты при соответствующих слагаемых многочлена выводятся во вторую таблицу. При изменении степени, многочлен пересчитывается автоматически, и все изменения отображаются на графике и в таблицах.

Кнопка «МНК 2» без пометки «Авто» запускает алгоритм поиска аппроксимирующей функции методом наименьших квадратов с базисными функциями, выбранными в третьей таблице (количество, порядок, комбинация и дополнительные параметры выбираются любыми, но в случае линейной зависимости программа выдаст ошибку). После успешного выполнения алгоритма, результат выводится аналогично, но коэффициенты во второй таблице уже соответствуют коэффициентам базисных функций в самой аппроксимирующей функции.

Если при нажатии кнопки «МНК 2» стоит пометка «Авто», то выбор базисных функций и параметров для них определяется автоматически, путём перебора используемых различных комбинаций базисных функций и параметров. Сложность рассматриваемых комбинаций регулируется значением в поле «Степень». Критерием для выбора оптимальной конфигурации служит минимальное среднеквадратическое отклонение в узлах таблично заданной функции среди рассмотренных вариантов. Вывод результатов аналогичен режиму без автоматического подбора базисных функций, разница заключается в том, что оптимальный набор базисных функций появится в третьей таблице автоматически.

Нажатие кнопки «Доп точки Берга» запускает алгоритм Берга и позволяет построить по нему заданное в поле «Точки» количество точек. В результате найденные точки появятся в четвёртой таблице и отобразятся на графике.

Если после построения точек методом Берга построить аппроксимирующую функцию, то построение будет производиться с расчётом этих точек. Если это не нужно, то точки сбрасываются построением нуля точек методом Берга.

Для вывода аппроксимирующей функции предусмотрена кнопка «Вывести функцию в файл», с помощью которой найденная функция выводится в указанный файл в виде, представленном на рис. 2:

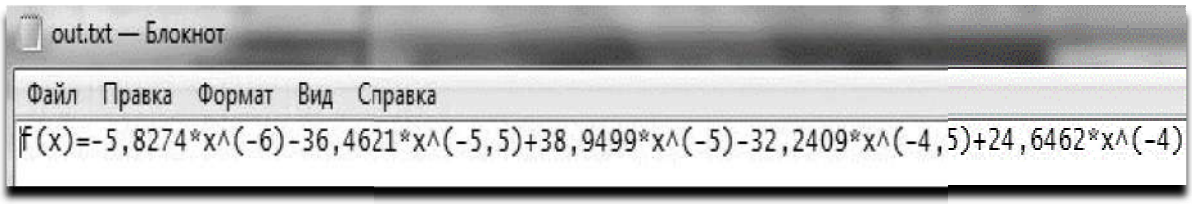

Рис. 2. Вид аппроксимирующей функции

Графики аппроксимирующих функций

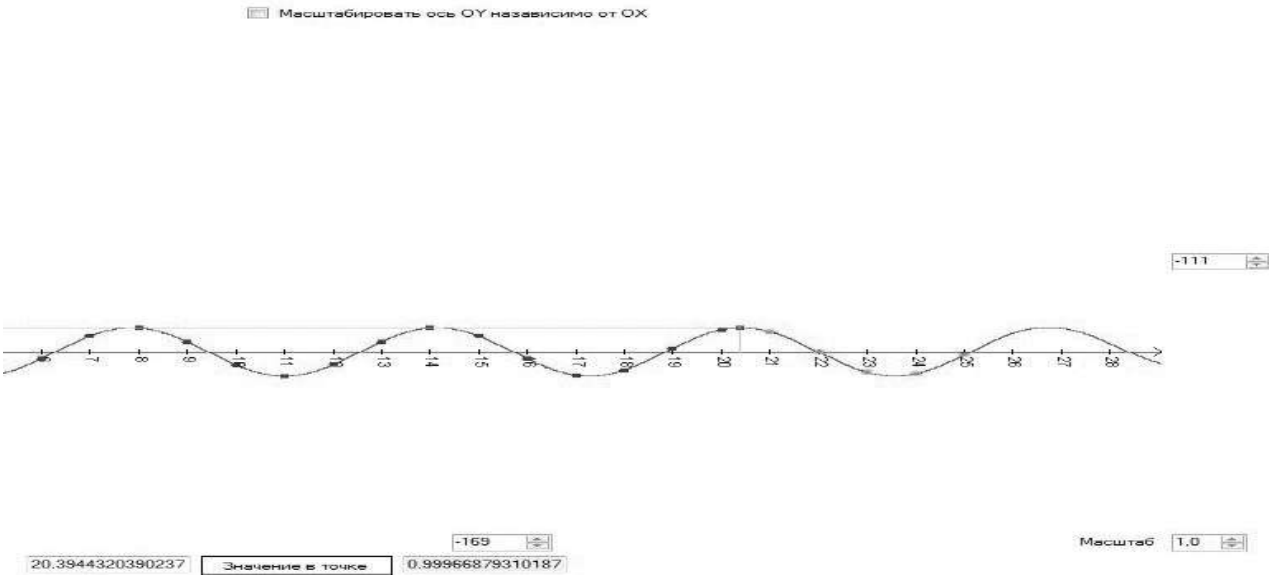

Рис. 3. Пример построенного графика аппроксимирующей функции

Программа предусматривает возможность построения графиков аппроксимирующих функций, которые демонстрируют характер ее изменения. Пример построения графика приведен на рис. 3. При вычислении заданного прогнозного значения оно указывается на графике аппроксимирующей функции. Блок схема рассматриваемого алгоритма приведена на рис. 4.

Примеры построения прогнозных моделей компьютерных инцидентов.

Далее в работе приведен пример построения прогнозной модели интенсивности компьютерных инцидентов. В табл. 2 приведены данные о количестве инцидентов, зафиксированных в российских ИТ – компаниях в период с января по май 2020 года, взятые с сайта компании *Positive Technologies* [11].

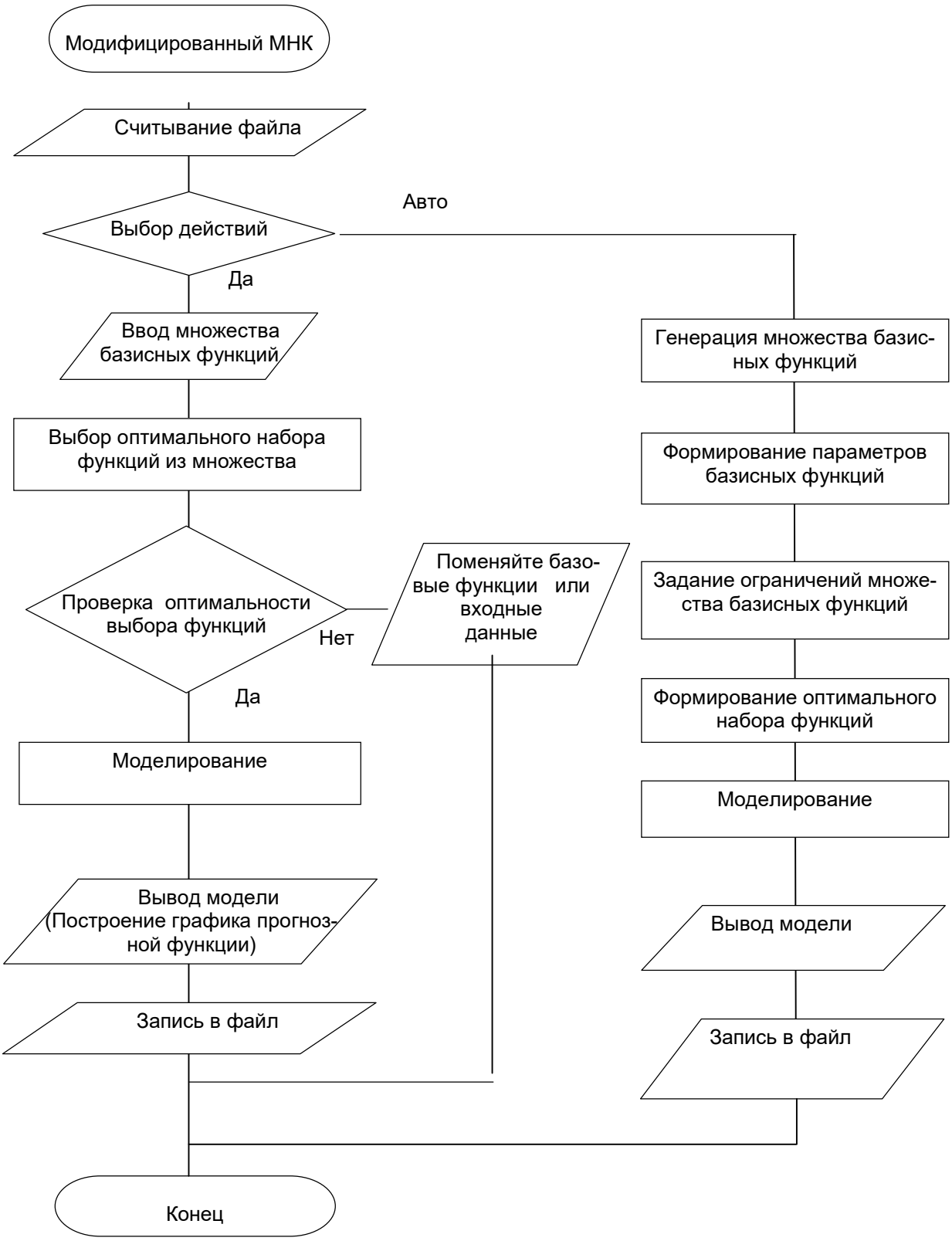

Рис. 4. Блок-схема алгоритма на основе модифицированного МНК

Таблица 2

Динамика появления компьютерных инцидентов

№	*Период*	*Количество инцидентов*
1	01.2020	167
2	02.2020	194
3	03.2020	160
4	04.2020	202
5	05.2020	206

Построенная по этим данным непрерывная аппроксимирующая функция *f(x)* имеет вид:

$$f(x) = 208.5179 - 6.2240 \cdot \cos 3x - 17.1202 \cdot x^{-2} - 36.2834 \cdot x^{-0.5} - \\ -27.7330 \cdot \cos 4x + 15.4545 \cdot \sin 4x. \quad (6)$$

График функции *f (x)* представлен на рис. 5.

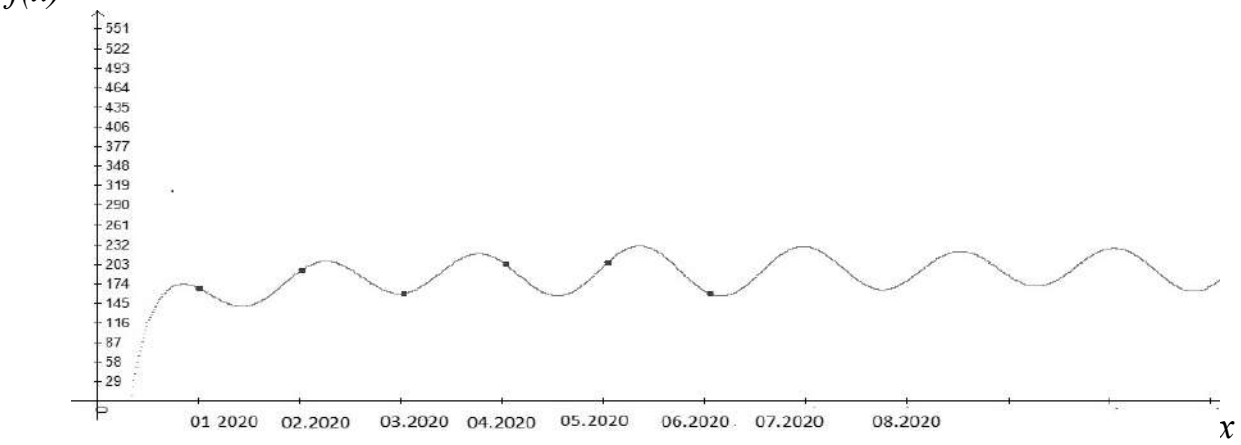

Рис. 5. График функции *f(x)*

В табл. 3 представлены прогнозные значения, полученные с помощью аппроксимирующей функции *f(x)*.

Таблица 3

Прогноз появления инцидентов

№	*Период*	*Количество инцидентов*	№	*Период*	*Количество инцидентов*
1	01.2020	167	11	11.2020	225
2	02.2020	194	12	12.2020	170
3	03.2020	160	13	01.2021	204
4	04.2020	202	14	02.2021	216
5	05.2020	206	15	03.2021	169
6	06.2020	159	16	04.2021	217
7	07.2020	163	17	05.2021	206
8	08.2020	228	18	06.2021	168
9	09.2020	178	19	07.2021	235
10	10.2020	186	20	08.2021	180

Пример вычисления параметра T_0.

В заключение работы, с использованием полученных результатов, рассмотрим пример вычисления параметра T_0 – времени безопасной работы информационной системы.

Обозначим через N - количество информационных систем, участвующих в приведенной выше статистике инцидентов и, будем считать, что материальный ущерб от реализации каждого инцидента одинаков и равен u.

Тогда, функция рисков $R(t)$ для одной информационной системы имеет вид

$$R(t) = \frac{f(t) \cdot u}{N} \quad . \tag{7}$$

где $f(t) = f(x)$ при переходе к временным характеристикам.

В соответствии с (6) функцию $f(t)$ можно представить в виде:

$$f(t) = \alpha_1 - \alpha_2 \cdot \cos 3t - \alpha_2 \cdot t^{-2} - \alpha_3 \cdot t^{-0.5} - \alpha_4 \cdot \cos 4t + \alpha_5 \cdot \sin 4t,$$

где $\alpha_1,...,\alpha_5$ - соответствующие числовые коэффициенты.

Заметим далее, что имеет место очевидное неравенство:

$$f(t) \le \alpha_6 + 4 \cdot \alpha_5 \cdot t,$$

где $\alpha_6 = \alpha_1 + ... + \alpha_4$, $t \ge 0$.

Тогда значение величины T_0 – времени безопасной работы информационной системы, может быть найдено из соотношения:

$$T_0 = \frac{R_0 \cdot N - \alpha_6 \cdot u}{4 \cdot \alpha_5 \cdot u}$$

При задании значений величин R_0 – допустимой границы потерь, N – числа информационных систем и u - ущерба при реализации инцидентов из последнего соотношения может быть получено значение величины T_0.

Заключение

В настоящей статье исследуются вопросы применения риск-ориентированного подхода к оценке защищенности информационных систем. Изложен подход, предусматривающий зависимость параметров риска от времени и предложен метод построения непрерывных прогнозных функций, описывающих возможные сценарии развития событий. Дано подробное описание методики построения указанных функций и методики определения защищенности ИС. Приведена блок схема алгоритма и дано подробное описание интерфейса программы, позволяющей строить непрерывные прогнозные функции и, в качестве иллюстрации предлагаемой методики, рассмотрен пример подхода к оценке защищенности ИС на основе данных об инцидентах, имевших место в российских ИТ-компаниях.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 13335-1:2006. Информационные технологии. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

2. ГОСТ Р ИСО/МЭК 13335-3:2007. Информационные технологии. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий.

3. ГОСТ Р ИСО/МЭК 13335-5:2007. Информационные технологии. Методы и средства обеспечения безопасности. Руководство по менеджменту безопасности сети.

4. *Лось А. Б. Кабанов А. С., Трунцев В. И.* Временная модель оценки риска нарушения информационной безопасности // Доклады ТУСУР. Томск. 2012. № 1. Ч. 2. С. 87-91.

5. *Ермакова А. Ю., Лось А. Б.* Построение модели ущерба активам организации при возникновении инцидентов, приводящих к нарушению информационной безопасности // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками: сборник статей Междунар. науч.-практич. конференции. 2020. С. 77−85.

6. *Ермакова А. Ю., Радько Н. М., Плотников Д. Г.* Модель управления рисками информационной безопасности при нарастающей величине ущерба // Промышленные АСУ и контроллеры. 2021. № 8. С. 48−55.

7. *Остапенко А. Г.* К вопросу об оценке ущерба в жизнестойкости атакуемых распределенных информационных систем: Развитие методического обеспечения // Информация и безопасность. 2012. № 4. С. 583 – 584.

8. *Ермакова А. Ю. Лось А. Б.* Исследование прогнозных моделей динамической системы на примере прогноза инцидентов информационной безопасности // Компьютерные науки и информационные технологии: сборник статей Международной научно-практической конференции. 2018. С. 144−149.

9. *Ермакова А. Ю.* Об оценке точности прогнозирования состояния динамической системы методом построения аппроксимирующих функций // Промышленные АСУ и контроллеры. 2018. № 5. С. 36−42.

10. *Ермакова А. Ю.* Об одном подходе к оценке защищенности информационной системы на основе анализа инцидентов // Системы высокой доступности. 2018. № 4. С. 32−35.

11. Сайт компании Positive Technologies. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/ (дата обращения 17.08.2021).