ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-3-72-82 Оригинальная статья /Original article

CC BY 4.0

Прогнозирование количества выявляемых уязвимостей информационной безопасности на основе теории «серых систем»

А.О. Ефимов, С.А. Мишин, Е.А. Рогозин
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Целью работы является оценка возможности применения теории «серых систем» для построения методики прогнозирования количества выявляемых уязвимостей в условиях неопределенности воздействующих факторов и недостатка исходных данных, включая сравнительный анализ результатов указанного прогнозирования, полученных с помощью традиционной и улучшенной моделей теории «серых систем», а также модели машинного обучения. **Метод.** В работе описывается методика построения «серой модели» прогнозирования количества выявляемых уязвимостей на основе теории «серых систем». Исходными данными для прогнозирования является информация, получаемая из базы данных уязвимостей CVE (Common Vulnerabilities and Exposures). Анализируются результаты прогнозирования, полученные при использовании разработанной «серой модели» и модели линейной регрессии, реализованной на базе библиотеки scikit-learn и языка программирования Python. **Результат.** Применение модели линейной регрессии и моделей, построенных на базе теории «серых систем», для прогнозирования количества выявляемых уязвимостей позволяет получить близкие значения прогноза. Согласно данным, полученным из базы данных уязвимостей CVE, за 1 квартал 2023 года опубликована информация о 7015 выявленных уязвимостях. Ближе всего к опубликованному значению оказался прогноз, полученный на основе традиционной модели теории «серых систем». Прогноз «серой модели» построен лишь на значениях исходных данных и не зависит от обстоятельств, возникающих в сфере информационной безопасности, что является ограничением в использовании предлагаемой методики. **Вывод.** Результаты проведенного исследования свидетельствуют о возможности применения теории «серых систем» для краткосрочного прогнозирования количества обнаруживаемых уязвимостей. Применение разработанной методики позволяет осуществлять указанное прогнозирование с ограниченным числом исходных данных.

Ключевые слова: информационная безопасность, защита информации, серые системы, количество уязвимостей, уязвимость, прогнозирование.

Для цитирования: А.О. Ефимов, С.А. Мишин, Е.А. Рогозин. Прогнозирование количества выявляемых уязвимостей информационной безопасности на основе теории «серых систем». Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3):72-82. DOI:10.21822/2073-6185-2023-50-3-72-82

Forecasting the number of identified information security vulnerabilities based on the theory of “Gray Systems”

A.O. Efimov, S.A. Mishin, E.A. Rogozin
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov St., Voronezh 394065, Russia

Abstract. **Objective**. The aim of the work is to assess the possibility of applying the theory of “gray systems” to build a methodology for predicting the number of identified vulnerabilities in conditions of uncertainty of influencing factors and lack of initial data, including a comparative analysis of the results of this prediction obtained using traditional and improved models of the theory of “gray systems”, as well

as machine learning models. **Method**. The paper describes a technique for constructing a "gray model" for predicting the number of identified vulnerabilities based on the theory of "gray systems". The initial data for forecasting is information obtained from the CVE (Common Vulnerabilities and Exposures) vulnerability database. In the course of the study, the results of forecasting obtained using the developed "gray model" and the linear regression model implemented on the basis of the scikit-learn library and the Python programming language are analyzed. **Result**. The use of a linear regression model and models based on the theory of "gray systems" to predict the number of identified vulnerabilities allows you to get close forecast values. According to data obtained from the CVE vulnerability database, information on 7,015 identified vulnerabilities was published for the 1st quarter of 2023. The forecast obtained on the basis of the traditional model of the theory of "gray systems" turned out to be the closest to the published value. It should be noted that the forecast of the "gray model" is based only on the values of the initial data and does not depend on the circumstances arising in the field of information security, which is a limitation in the use of the proposed methodology. **Conclusion**. The results of the study indicate the possibility of applying the theory of "gray systems" for short-term forecasting of the number of detected vulnerabilities. The application of the developed methodology makes it possible to carry out the specified forecasting with a limited number of initial data.

Keywords: information security, protection of information, gray systems, number of vulnerabilities, vulnerability, forecasting.

For citation: A.O. Efimov, S.A. Mishin, E.A. Rogozin. Forecasting the number of identified information security vulnerabilities based on the theory of "Gray Systems". Herald of Daghestan State Technical University. Technical Science. 2023; 50(3):72-82. DOI:10.21822/2073-6185-2023-50-3-72-82

Введение. Область выявления уязвимостей обладает достаточно высокой степенью неопределенности. В свою очередь, решение задачи прогнозирования количества уязвимостей поможет уменьшить указанную неопределенность тем самым повысить эффективность подготовки специалистов информационной безопасности. В связи с этим тема исследования является актуальной.

Постановка задачи. Предложенная в статье методика прогнозирования количества выявляемых уязвимостей разработана на основе работы Ван Ю. «Прогнозирование объемов перевозок пассажиров на основе теории «серых систем»», опубликованной в Вестнике Белорусского государственного университета транспорта: наука и транспорт [1]. Теоретическим базисом данной работы является статья «Introduction to Grey System Theory», опубликованная Deng Julong в 1989 году [2].

Применение теории «серых систем» для задач прогнозирования обладает рядом преимуществ: работа с небольшим количеством исходных данных, характеризующих изучаемые процессы или объекты, учет тенденции их поведения и связей между ними, низкая ресурсоемкость и простота использования, возможность использования в дополнение к другим методам прогнозирования [1,2]. Однако у рассматриваемой теории есть и ряд недостатков: невозможность учета внешних факторов, влияющих на исследуемую систему, неточность прогнозов в долгосрочной перспективе [1,2]. В качестве исходных данных будут взяты сведения о количестве выявленных уязвимостей за несколько лет, отраженных в базе данных уязвимостей CVE [3].

Таблица 1. Исходные данные количества выявленных уязвимостей (база данных уязвимостей CVE)

Table 1. Initial data on the number of identified vulnerabilities (CVE database)

	2019г.	2020г.	2021г.	2022г.
Количество обнаруженных уязвимостей/ Number of vulnerabilities discovered (I,II,III,IV квартал)	3245, 4590, 5150, 4822	4807, 5011, 4170, 4387	4415, 5005, 5541, 5200	6015, 6365, 6448, 6231

Из табл. 1 видно, что в исходных данных присутствует тенденция к росту количества обнаруживаемых уязвимостей.

Методы исследования. Модель GM (Grey Model) – это дифференциальное уравнение «серой модели» прогнозирования. Дифференциальное уравнение первого порядка с N переменными может быть представлена как GM (1, N). Таким же образом дифференциальное уравнение с одной переменной первого порядка представляется как GM (1, 1). Модель GM (1, 1) является самой простой и основной моделью серого прогнозирования [1,2].

На первом этапе построения «серой модели» прогнозирования производится сбор (поиск информации о количестве обнаруженных уязвимостей за рассматриваемый период времени), подготовка (количество обнаруженных уязвимостей представляется в виде временного ряда с равными интервалами времени) и проверка исходных данных на соответствие требованиям теории «серых систем» [1].

Последовательность исходных данных представляется следующим образом:

$$x^{(0)} = \{x^{(0)}(1), x^{(0)}(2) \dots, x^{(0)}(n)\} \quad (1)$$

Важно отметить, что элементы последовательности могут иметь только положительное значение. После построения исходной последовательности данных, производится расчет параметров статистического ряда и проверка их сглаженности:

$$\beta(k) = \frac{x^{(0)}(k-1)}{x^{(0)}(k)}, k = 3, 4, \dots, n, \quad (2)$$

где k – порядковый номер элемента, начиная с 3 до n (количество элементов исходной последовательности данных).

Если коэффициенты связности находятся в диапазоне $(e^{-2/(n+1)}, e^{2/(n+1)})$, то исходные данные соответствуют модели GM (1, 1) и пригодны для использования в прогнозировании [1]. В ином случае необходима дополнительная обработка данных, с помощью методов наименьших квадратов, логарифмирования и др. [1].

Хорошая сглаженность данных позволяет получить более точные результаты их анализа и прогнозирования, так как в таком ряду проще выявлять закономерности и тренды. Тем не менее, необходимо учитывать, что сглаживание данных может привести к потере некоторой информации (определенных деталей в данных). Поэтому необходимо искать компромисс между достаточной сглаженностью и сохранением исходной информации, чтобы получить наиболее точный и полезный результат прогнозирования.

После проведения описанной выше подготовки данных генерируется новый набор данных, расширяющий исходную последовательность:

$$x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i), k = 1,2,3 \dots n. \quad (3)$$

$$x^{(1)} = \{x^{(1)}(1), x^{(1)}(2) \dots, x^{(1)}(n)\} \quad (4)$$

После построения последовательности данных, которая включает в себя промежутки времени и зарегистрированные значения обнаруженных уязвимостей, производится проверка ее подчинения экспоненциальному закону распределения, используя следующее выражение [1-2, 4-15]:

$$\sigma^{(1)}(k) = \frac{x^{(1)}(k)}{x^{(1)}(k-1)}, k = 3, 4, \dots, n. \quad (5)$$

Результатом данной проверки является ответ на вопрос: «Является ли изменение значения величины во времени экспоненциальным?». Если существует $\sigma^{(1)}(k) \in [1, 1 + \delta]$, где δ обычно принимают равным 0,5, то последовательность $x^{(1)}$ удовлетворяет экспоненциальному закону распределения. В противном случае выборка должна быть расширена [1]. В случае если изменение подчиняется экспоненциальному закону, то делается вывод о том, что исходные данные могут быть использованы для построения «серой модели».

Таким образом, применение модели GM (1, 1) позволяет не только сгладить данные, но и прогнозировать их изменение во времени на основе экспоненциального закона убывания

или роста.

При подчинении последовательности $x^{(1)}$ экспоненциальному закону распределения, можно предположить, что последовательность $x^{(1)}$ удовлетворяет условиям линейного дифференциального уравнения первого порядка [1]:

$$\frac{dx^{(1)}}{dx} + ax^{(1)} = u, \tag{6}$$

где a – коэффициент регрессии, отражающий тенденцию изменения исходных данных $x^{(0)}$ и новую последовательность данных $x^{(1)}$, которая является параметром построения модели; u – коэффициент согласованности, отражающий взаимосвязь между данными модели.

Согласно исходной методике [1], дифференциальное уравнение модели примет следующий вид:

$$x^{(0)}(k) = -aZ^{(1)}(k) + u, \tag{7}$$

где, $Z^{(1)}$ – это сгенерированная последовательность, смежная с последовательностью, полученной на основе исходных данных, обозначенной как $x^{(1)}$.

$$Z^{(1)}(k) = 0{,}5\left[x^{(1)}(k) + x^{(1)}(k-1)\right], k = 2, 3, \dots n. \tag{8}$$

Далее из ранее полученных данных производится построение матриц Y_n, B и определение параметров a, u:

$$\begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \dots \\ x^{(0)}(n) \end{bmatrix} = \begin{bmatrix} -Z^{(1)}(2) & 1 \\ -Z^{(1)}(3) & 1 \\ \dots & \dots \\ -Z^{(1)}(n) & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ u \end{bmatrix} \tag{9}$$

$$Y_n = [x^{(0)}(2), x^{(0)}(3), \dots, x^{(0)}(n)]^{\mathrm{T}} \tag{10}$$

$$B = \begin{bmatrix} -Z^{(1)}(2) & 1 \\ -Z^{(1)}(3) & 1 \\ \dots & \dots \\ -Z^{(1)}(n) & 1 \end{bmatrix} \tag{11}$$

$$\hat{a} = \begin{bmatrix} a \\ u \end{bmatrix} \tag{12}$$

Определение $\hat{a}$ производится методом наименьших квадратов, следующим образом:

$$\hat{a} = \begin{bmatrix} a \\ u \end{bmatrix} = (B^{\mathrm{T}}B)^{-1}B^{\mathrm{T}}Y_n. \tag{13}$$

Метод наименьших квадратов позволяет оценить параметры модели, которые являются оптимальными при минимальной сумме квадратов отклонений между моделью и исходными данными. Таким образом, применение данного метода в теории «серых систем» позволяет улучшить точность прогнозирования, устранить некоторые ошибки и сделать модель более стабильной.

Подставляя значения (a, u) в линейное дифференциальное уравнение первого порядка, получаем модель функции времени отклика модели:

$$\tilde{x}^{(0)} = \left[\tilde{x}^{(1)} - \frac{u}{a}\right]e^{-at} + \frac{u}{a}, k = 1, 2, 3, \dots n. \tag{14}$$

При восстановлении исходного состояния данных и использовании параметров u, a модель прогнозирования может быть представлена следующим образом:

$$\tilde{x}^{(0)}(k+t) = x^{(1)}(k+t) - x^{(1)}(k) = (e^{-a} - 1)\left[x^{(0)}(1) - \frac{u}{a}\right]e^{ak} \tag{15}$$

Полученная модель прогнозирования представляет собой сглаженную экспоненциальную кривую, которая снижает неопределенность исходных данных [1].

Точность прогноза может быть оценена с помощью сравнения прогнозных значений с реальными данными, которые становятся доступными после периода прогнозирования. Также в первоисточнике, автор приводит методику построения улучшенной модели прогнозирования, которая позволяет устранить неотъемлемые отклонения от традиционной модели и расширить диапазон ее применения [1]. Недостатком улучшенной модели прогнозирования является невозможность предсказания на ее основе уровня неопределенности данных [1]. Построение улучшенной модели прогнозирования может быть выполнено на основе параметров a и u, уже использовавшихся ранее:

$$\eta = \ln\frac{2-a}{2+a},\ M = \frac{2u}{2+a}. \quad (16)$$

На основе найденных параметров η и M улучшенная модель прогнозирования будет иметь вид:

$$\hat{x}^{(0)}(1) = x^{(0)}(1); \quad (17)$$

$$\hat{x}^{(0)}(k) = M * e^{-\eta(k-1)}, k = 2, 3, \dots, n. \quad (18)$$

В целях полноты анализа получаемых результатов в рамках проведенного исследования использованы как традиционная так и улучшенная модели прогнозирования.

Прогнозирование количества выявленных уязвимостей с использованием традиционной и улучшенной моделей прогнозирования на основе сведений базы данных уязвимостей CVE. Определим последовательность исходных данных:

$$x^{(0)} = \{3245, 4590, 5150, 4822, 4807, 5011, 4170, 4387, 4415, 5005, 5541, 5200, 6015, 6365, 6448, 6231\}$$

По формуле (2) рассчитаем коэффициенты гладкости данных, и сведем их в табл. 2:

Таблица 2. Рассчитанные коэффициенты сглаженности данных
Table 2. Calculated data smoothing coefficients

k	$\beta(k)$
3	0,8913
4	1,0680
5	1,003
6	0,9592
7	1,2016
8	0,9505
9	0,9936
10	0,8821
11	0,9032
12	1,0655
13	0,8645
14	0,9450
15	0,9871
16	1,0348

Диапазон значений заданного набора исходных данных с некоторой погрешностью входит в необходимый диапазон значений $\beta(k) \in [0.88, 1.12]$.

В целях максимального сохранения объема исходных данных примем, что все значения удовлетворяют требованиям, и не требуют дополнительной обработки перед использованием.

На основе формул (3) и (4) сгенерируем новую последовательность данных:

$$x^{(1)} = \{3245, 7835, 12985, 17807, 22614, 27625, 31795, 36182, 40597, 45602, 51143, 56343, 62358, 68723, 75171, 81402\}$$

Результаты проверки подчинения изменения величин сгенерированной последовательности $x^{(1)}$ экспоненциальному закону распределения (5) приведем в табл. 3: Полученные значения $\sigma^{(1)}(k)$ (табл. 3), а также пояснения к (5) позволяют сделать следующий вывод: исходные данные могут быть положены в основу построения «серой модели» прогнозирования.

Таблица 3. Проверка подчинения сгенерированной последовательности $x^{(1)}$ экспоненциальному закону распределения

Table 3. Checking the subordination of the generated sequence $x^{(1)}$ to the exponential distribution law

k	$\sigma^{(1)}(k)$
3	1,6573
4	1,3713
5	1,2699
6	1,2215
7	1,1509
8	1,1379
9	1,1220
10	1,1232
11	1,1215
12	1,1016
13	1,1067
14	1,1020
15	1,0938
16	1,0828

Произведем генерацию последовательности на основе $x^{(1)}$ (8):

$$Z^{(1)} = \{5540,10410,15396,20210,25119,29710,33988,38389,\\ 43101,48374,53743,59350,65540,71947,78286\}$$

На основе полученных данных сформируем матрицы:

$$\begin{bmatrix}4590\\5150\\4822\\4807\\5011\\4170\\4387\\4415\\5005\\5541\\5200\\6015\\6365\\6448\\6231\end{bmatrix} = \begin{bmatrix}-5540 & 1\\-10410 & 1\\-15396 & 1\\-20210 & 1\\-25119 & 1\\-29710 & 1\\-33988 & 1\\-38389 & 1\\-43101 & 1\\-48374 & 1\\-53743 & 1\\-59350 & 1\\-65540 & 1\\-71947 & 1\\-78286 & 1\end{bmatrix} \cdot \begin{bmatrix}a\\u\end{bmatrix}$$

$$Y_n = [4590,5150,4822,4807,5011,4170,4387,\\ 4415,5005,5541,5200,6015,6365,6448,6231]^{\mathrm{T}}$$

$$B = \begin{bmatrix}-5540 & 1\\-10410 & 1\\-15396 & 1\\-20210 & 1\\-25119 & 1\\-29710 & 1\\-33988 & 1\\-38389 & 1\\-43101 & 1\\-48374 & 1\\-53743 & 1\\-59350 & 1\\-65540 & 1\\-71947 & 1\\-78286 & 1\end{bmatrix}$$

На основе формулы (13), получаем значения коэффициента регрессии a = -0,026 и коэффициента согласованности u = 4178. Подставив значения в формулу (15), получаем набор прогнозируемых значений, рассчитанных на основе традиционной модели прогнозирования (табл.4).

Таблица 4. Прогноз количества выявленных уязвимостей на основе традиционной модели
Table 4. Prediction of the number of identified vulnerabilities according to the traditional model

Квартал, год/ Quarter, year	Количество выявленных уязвимостей/ Number of identified vulnerabilities	Прогноз количества выявленных уязвимостей/ Forecast of the number of identified vulnerabilities
1, 2019	3245	4431
2, 2019	4091	4547
3, 2019	5150	4666
4, 2019	4822	4788
1, 2020	4807	4913
2, 2020	5011	5042
3, 2020	4170	5174
4, 2020	4387	5309
1, 2021	4415	5448
2, 2021	5005	5591
3, 2021	5541	5737
4, 2021	5200	5888
1, 2022	6015	6042
2, 2022	6365	6200
3, 2022	6448	6362
4, 2022	6231	6529
1, 2023	-	6700
2, 2023	-	6875
3, 2023	-	7055
4, 2023	-	7240
1, 2024	-	7429
2, 2024	-	7624
3, 2024	-	7823
4, 2024	-	8028

Построение улучшенной модели может быть произведено на основе параметров *a, u*, полученных ранее (16-18).

Воспользовавшись указанными параметрами, построим усовершенствованную модель:

$$\eta = \ln\frac{2-a}{2+a} = -0{,}0260015;\ M = \frac{2u}{2+a} = 4233{,}02938.$$

$$\hat{x}^{(0)}(1) = 3245;$$

$$\hat{x}^{(0)}(k) = 4233{,}02938 * e^{0{,}0260015*(k-1)}, k = 2, 3, \dots, n.$$

Произведем прогнозирование на основе полученной усовершенствованной модели (табл. 5).

Для сравнения результатов, получаемых на основе применения построенных «серых моделей» и известных методов прогнозирования, дополнительно построена модель прогнозирования на основе метода линейной регрессии, реализованного в библиотеке машинного обучения scikit-learn.

Обучение модели происходило на тех же исходных данных, что и при построении «серых моделей».

В результате применения обученной модели прогнозирования на основе линейной регрессии получен прогноз количества выявленных уязвимостей, представленный в табл. 6.

Таблица 5. Прогноз количества выявленных уязвимостей на основе усовершенствованной модели

Table 5. Forecast of the number of identified vulnerabilities according to the improved model

Квартал, год/Quarter, year	Количество выявленных уязвимостей/ Number of identified vulnerabilities	Прогноз количества выявленных уязвимостей/ Forecast of the number of identifiedvulnerabilities
1, 2019	3245	3245
2, 2019	4091	4345
3, 2019	5150	4459
4, 2019	4822	4576
1, 2020	4807	4697
2, 2020	5011	4821
3, 2020	4170	4948
4, 2020	4387	5078
1, 2021	4415	5212
2, 2021	5005	5349
3, 2021	5541	5490
4, 2021	5200	5635
1, 2022	6015	5783
2, 2022	6365	5935
3, 2022	6448	6092
4, 2022	6231	6252
1, 2023	-	6417
2, 2023	-	6586
3, 2023	-	6759
4, 2023	-	6938
1, 2024	-	7120
2, 2024	-	7308
3, 2024	-	7500
4, 2024	-	7698

Таблица 6. Прогноз количества выявленных уязвимостей с использованием метода линейной регрессии

Table 6. Prediction of the number of identified vulnerabilities using linear regression

Квартал, год/Quarter, year	Количество выявленных уязвимостей/ Number of identified vulnerabilities	Прогноз количества выявленных уязвимостей/ Forecast of the number of identifiedvulnerabilities
1, 2019	3245	3974
2, 2019	4091	4122
3, 2019	5150	4271
4, 2019	4822	4419
1, 2020	4807	4568
2, 2020	5011	4716
3, 2020	4170	4865
4, 2020	4387	5013
1, 2021	4415	5162
2, 2021	5005	5310
3, 2021	5541	5459
4, 2021	5200	5607
1, 2022	6015	5755
2, 2022	6365	5904
3, 2022	6448	6053
4, 2022	6231	6201
1, 2023	-	6350
2, 2023	-	6498
3, 2023	-	6647
4, 2023	-	6795
1, 2024	-	6944
2, 2024	-	7092
3, 2024	-	7241
4, 2024	-	7389

Обсуждение результатов. В целях проведения сравнительного анализа результатов прогнозирования, полученных с помощью традиционной и улучшенной «серой модели» прогнозирования, а также модели прогнозирования на основе линейной регрессии, разместим их в одной координатной плоскости и представим в виде графика (рис. 1).

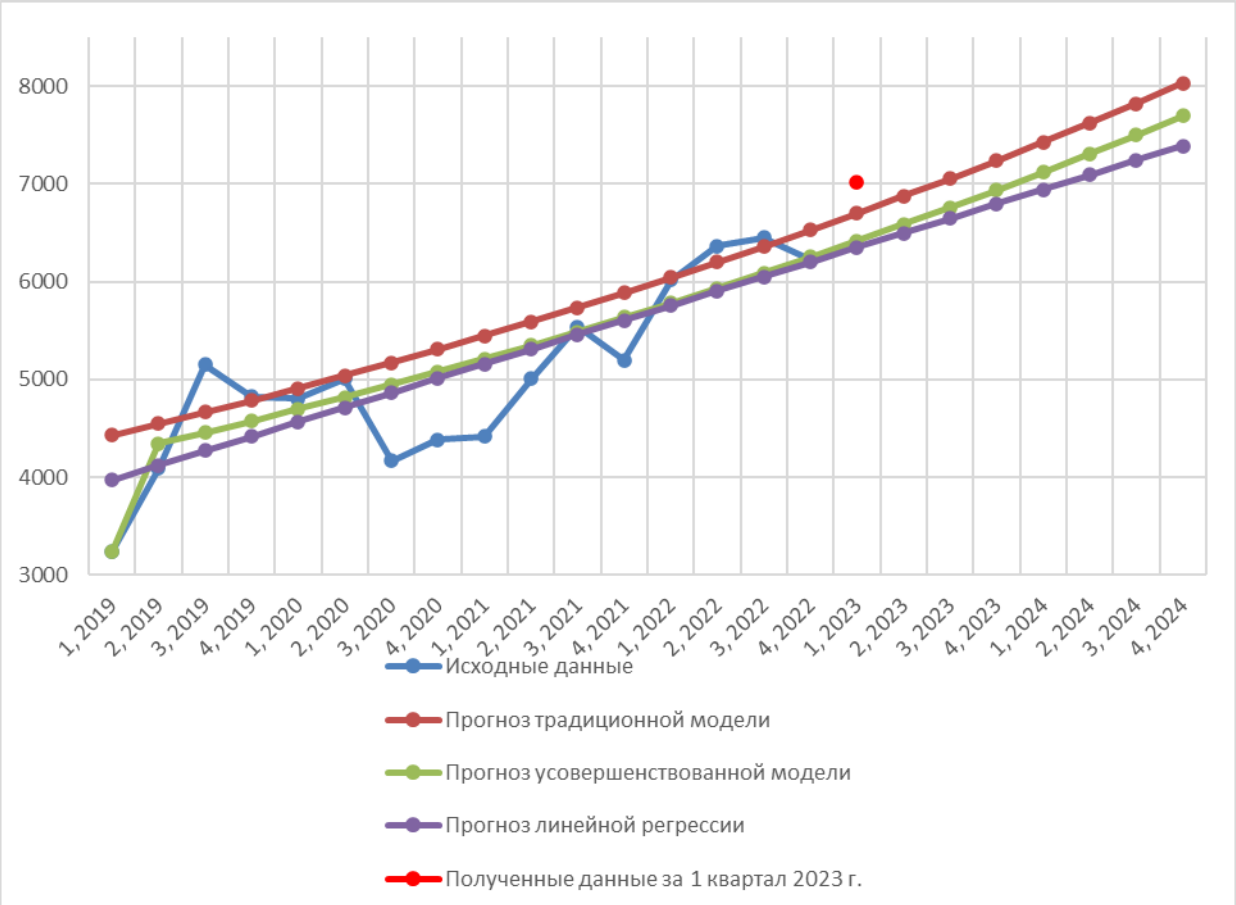

Рис. 1. График с результатами прогнозирования (расчет по данным CVE).
Fig. 1. A graph with the results of forecasting (calculation based on CVE data).

В результате анализа полученных в ходе прогнозирования значений, установлено: тенденция роста количества выявляемых уязвимостей в будущем будет сохранена; построенные модели прогнозирования содержат схожий тренд. Прогнозирование с применением метода линейной регрессии позволило получить схожие результаты с применением моделей, построенных на основе теории «серых систем».

Возможно, что при использовании большего числа данных в будущем качество прогнозирования может быть повышено.

Следует отметить, полученный прогноз основывается лишь на значениях исходных данных и не зависит от обстоятельств, возникающих в сфере информационной безопасности, что является явным недостатком приведенной методики.

Кроме указанного недостатка применение разработанных моделей на основе теории «серых систем» возможно только для краткосрочного прогнозирования и не позволяет получать ретроспективные данные, о чем свидетельствует график на рис. 1.

Согласно данным за 1 квартал 2023 года опубликована информация о 7015 выявленных уязвимостях [3]. Ближе всего к этому значению оказался прогноз данный традиционной «серой моделью» (6700).

Вывод. В случае отсутствия более точной методики прогнозирования приведенный в работе математический аппарат может быть использован для проведения прогноза при отсутствии информации о факторах, влияющих на изучаемые процессы.

Произведено прогнозирование количества уязвимостей на ближайшие два года. Но, как было сказано ранее, факторы, которые могут оказать серьезное воздействие на количество выявляемых уязвимостей в этот период времени, при проведении прогнозирования не учитываются. Построение прогноза на основе сведений, полученных от других компетентных организаций в области информационной безопасности, может дать отличающийся результат из-за сильного различия исходных данных [7,9,10].

Таким образом, использование теории «серых систем» для решения задач в области информационной безопасности требует проведения дальнейших исследований.

Библиографический список:

1. Ван, Ю. Прогнозирование объемов перевозок пассажиров на основе теории «серых систем» / Ю. Ван // Вестник Белорусского государственного университета транспорта: наука и транспорт. – 2021. – № 1(42). – С. 77-81. – EDN OKGSXG.
2. Deng, J. L. Introduction to grey system theory / J. L. Deng // J Grey System. - 1989; 1:1-24.
3. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org// (дата обращения: 01.03.2023).
4. Bindhu, B. K. Application of grey system theory on the influencing parameters of aerobic granulation in SBR / B. K. Bindhu, G. Madhu // Environ Technol. - 2017. - Sep; 38(17):2143-2152.
5. Дровникова И.Г., Етепнев А.С., Рогозин Е.А. Основные виды уязвимостей и взаимосвязь компонентов безопасности при обосновании показателей надёжности системы защиты информации от несанкционированного доступа в автоматизированных системах // Приборы и системы. Управление, контроль, диагностика. 2019. № 3. С. 59–64.
6. Кубарев, А. В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков / А. В. Кубарев // Вопросы кибербезопасности. – 2013. – № 2(2). – С. 29-33. – EDN SZEDHH.
7. База данных уязвимостей. ФСТЭК России. URL: https://bdu.fstec.ru/vul (дата обращения: 04.03.2023).
8. Коноваленко, С. А. Выявление уязвимостей информационных систем посредством комбинированного метода анализа параметрических данных, определяемых системами мониторинга вычислительных сетей / С. А. Коноваленко, И. Д. Королев // Альманах современной науки и образования. – 2016. – № 11(113). – С. 60-66. – EDN XEEDXH.
9. Карты источников, содержащих сведения об уязвимостях программного обеспечения / А. Л. Сердечный, М. А. Тарелкин, А. А. Ломов, К. В. Симонов // Информация и безопасность. – 2019. – Т. 22, № 3. – С. 411-422. – EDN ZOUMGN.
10. Федорченко, А. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей / А. В. Федорченко, А. А. Чечулин, И. В. Котенко // Информационно-управляющие системы. – 2014. – № 5(72). – С. 72-79. – EDN SXXXKH.
11. Сердечный А.Л.,. Герасимов И.В,. Макаров О.Ю и др. Технология выявления сведений об уязвимостях сторонних компонентов программного обеспечения с открытым исходным кодом. Информация и безопасность. 2020, т. 23, № 3, с. 347–364. DOI: http://dx.doi.org/10.36622/VSTU.2020.23.3.003. – EDN PYXOUT.
12. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения. Вопросы кибербезопасности. 2014, № 3(4), с. 20–28. – EDN SSYPXV.
13. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018, p. 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
14. Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
15. Lin G., Wen S., Han Q. -L., Zhang J. and Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020, vol. 108, no. 10, p. 1825–1848. DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.

References:

1. Wang, Yu. Forecasting passenger traffic volumes based on the theory of “gray systems” *Bulletin of the Belarusian State University of Transport: Science and Transport*. 2021;1(42): 77-81. – EDN OKGSXG. (In Russ)
2. Deng, J. L. Introduction to grey system theory. *J Grey System.* 1989; 1:1-24.
3. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org // (accessed 01.03.2023).
4. Bindhu, B. K. Application of grey system theory on the influencing parameters of aerobic granulation in SBR / B. K. Bindhu, G. Madhu. *Environ Technol*. 2017; 38(17):2143-2152.
5. Drovnikova I.G., Etepnev A.S., Rogozin E.A. Main types vulnerabilities and the relationship of security components in substantiating the reliability indicators of the information protection system against unauthorized access in automated systems. *Devices and systems. Management, control, diagnostics*. 2019; 3:. 59-64. (In Russ)
6. Kubarev, A.V. Approach to formalization of vulnerabilities of information systems based on their classification features. *Issues of cybersecurity*. 2013;2(2):29-33. – EDN SZEDHH. (In Russ)

7. Vulnerability database. FSTEC of Russia. URL: https://bdu.fstec.ru/vul (accessed: 03/04/2023).
8. Konovalenko, S. A. Identification of vulnerabilities of information systems by means of a combined method of analysis of parametric data determined by monitoring systems of computer networks. S. A. Konovalenko, I. D. Korolev. *Almanac of modern science and education*. 2016;1(113): 60-66. – EDN XEEDXH. (In Russ)
9. Maps of sources containing information about software vulnerabilities. A. L. Serdny, M. A. Tarelkin, A. A. Lomov, K. V. Simonov. *Information and security*. 2019; 22(3): 411-422. – EDN ZOUMGN. (In Russ)
10. Fedorchenko, A.V. Research of open databases of vulnerabilities and assessment of the possibility of their application in systems of security analysis of computer networks / A.V. Fedorchenko, A. A. Chechulin, I. V. Kotenko. *Information and control systems*. 2014; 5(72): 72-79. – EDN SXXXKH. (In Russ)
11. Serdechnyj A.L., Gerasimov I.V., Makarov O.YU. i dr. Technology for identifying information about vulnerabilities of third-party components of open source software. Informaciya i bezopasnost'. 2020;. 23(3):347–364 – EDN PYXOUT. (In Russ)
12. Avetisyan A.I., Belevancev A.A., Chuklyaev I.I. Technologies of static and dynamic analysis of software vulnerabilities. *Voprosy kiberbezopasnosti*. 2014; 3(4): 20–28 – EDN SSYPXV. (In Russ)
13. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018; 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
14. Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010; 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
15. Lin G., Wen S., Han Q. -L., Zhang J. and Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020;108(10):1825–1848. DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.

Сведения об авторах:

Ефимов Алексей Олегович, адъюнкт очной формы обучения; ea.aleksei@yandex.ru

Мишин Сергей Александрович, кандидат технических наук, доцент, заместитель начальника кафедры автоматизированных информационных систем органов внутренних дел; samishin@bk.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Information about authors:

Aleksey O. Efimov, full-time adjunct; ea.aleksei@yandex.ru

Mishin Sergey Alexandrovich, Candidate of Technical Sciences, Associate Professor, Deputy Head of the Department of Automated Information Systems of Internal Affairs Bodies; samishin@bk.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest

Поступила в редакцию/Received 05.07.2023.

Одобрена после рецензирования/ Reviced 31.07.2023.

Принята в печать/Accepted for publication 31.07.2023.