УДК: 004.056
doi: 10.26583/bit.2024.4.01

Сергей А. Будников[1], Михаил А. Тарелкин[2], Юрий К. Язов[3]
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»,
ул. 9 января, 280-а, Воронеж, 394036, Россия
[1]*e-mail: public.buser@bk.ru, https://orcid.org/https://0000-0003-2285-494X*
[2]*e-mail: mihail.tarelkin.93@mail.ru, https://orcid.org/0009-0006-1321-5416*
[3]*e-mail: yazoff_1946@mail.ru, https://orcid.org/0000-0001-8546-643X*

ПОДХОД К ПРОГНОЗИРОВАНИЮ СВОЙСТВ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. Разработан вероятностный подход к прогнозированию свойств выявляемых уязвимостей программного обеспечения. Подход основан на представлении процесса смены значений базовых метрик обнаруживаемых программных уязвимостей CVSS v3.0 в виде случайного марковского процесса с дискретными состояниями и непрерывным временем. При построении систем уравнений Колмогорова учитывалась динамика изменения средней интенсивности смены значений базовых метрик, зависящая от текущего времени. Получены аналитические линейные функции, аппроксимирующие средние значения мгновенной интенсивности смены значений базовых метрик в пределах квартала года, начиная с 1 января 2017 г. В интересах краткосрочного прогнозирования проведено вероятностное моделирование появления уязвимостей операционной системы Astra Linux Special Edition с заданными свойствами в виде значений базовых метрик CVSS v3.0 в зависимости от дня с момента обнаружения последней программной уязвимости. Начальными условиями моделирования установлены значения базовых метрик последней опубликованной программной уязвимости. Показана возможность расчета значений стационарных вероятностей появления заданных значений базовых метрик CVSS v3.0 уязвимостей для долгосрочного прогнозирования в течение года. Совпадение статистических данных за IV квартал 2023 г. и результатов моделирования процесса появления уязвимостей с этими свойствами подтвердили адекватность моделей и достоверность результатов прогнозирования. Областью применения разработанного подхода могут являться сфера разработки программного обеспечения и средств защиты информации, а также создаваемые и эксплуатируемые системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, линейная регрессия, марковский случайный процесс, оценка уязвимостей, прогнозирование, уравнения Колмогорова.
Для цитирования: БУДНИКОВ, Сергей А.; ТАРЕЛКИН, Михаил А.; ЯЗОВ, Юрий К. ПОДХОД К ПРОГНОЗИРОВАНИЮ СВОЙСТВ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Безопасность информационных технологий, [S.l.], т. 31, № 4, с. 31–43, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1713. DOI: http://dx.doi.org/10.26583/bit.2024.4.01.

Sergey A. Budnikov[1], Mikhail A. Tarelkin[2], Yuri K. Yazov[3]
Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control»,
January 9 str., 280-a, Voronezh, 394036, Russia
[1]*e-mail: public.buser@bk.ru, https://orcid.org/ https://0000-0003-2285-494X*
[2]*mihail.tarelkin.93@mail.ru, https://orcid.org/0009-0006-1321-5416*
[3]*e-mail: yazoff_1946@mail.ru, https://orcid.org/0000-0001-8546-643X*

An approach to predicting the properties of software vulnerabilities

Abstract. A probabilistic approach to predicting the properties of identified software vulnerabilities has been developed. The approach is based on representing the process of changing the values of the basic metrics of detected software vulnerabilities CVSS v3.0 as a random Markov process with discrete states and continuous time. When constructing systems of Kolmogorov equations, the dynamics of changes in the average intensity of changes in the values of basic metrics, depending on the current time, was taken into account. Analytical linear functions were obtained that approximate the average values of the instantaneous intensity of changes in the values of basic metrics within a quarter of the year, starting from January 1, 2017. In the interests of short-term forecasting, a probabilistic modeling of the emergence of vulnerabilities in the Astra Linux Special Edition operating system with specified properties in the form of values of basic CVSS v3.0 metrics was carried out depending on the day from the moment the last software vulnerability was discovered. The initial modeling conditions are set to the values of the basic metrics of the latest published software vulnerability. The possibility of calculating the values of stationary probabilities of occurrence of given values of the basic metrics of CVSS v3.0 vulnerabilities for long-term forecasting throughout the year is shown. Coincidence of statistical data for the fourth quarter of 2023. and the results of modeling the process of emergence of vulnerabilities with these properties confirmed the adequacy of the models and the reliability of the prediction results. The scope of application of the developed approach can be the sphere of software development and information security tools, as well as the created and operated systems for ensuring information security of significant objects of critical information infrastructure.

Keywords: critical information infrastructure, linear regression, Markov random process, vulnerability assessment, forecasting, Kolmogorov equations.

For citation: BUDNIKOV, Sergey A.; TARELKIN, Mikhail A.; YAZOV, Yuri K. An approach to predicting the properties of software vulnerabilities. IT Security (Russia), [S.l.], v. 31, no. 4, p. 31–43, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1713. DOI: http://dx.doi.org/10.26583/bit.2024.4.01.

Введение

Рост количества обнаруженных уязвимостей в информационных системах, информационно-телекоммуникационных сетях и автоматизированных системах управления в условиях резкого нарастания численности и мощности целенаправленных компьютерных атак требует наличия надежных подходов к прогнозированию уровня защищенности объектов критической информационной инфраструктуры (КИИ) Российской Федерации. Так, количество обнаруженных за второй квартал 2023 г. уязвимостей выросло на 7%, по сравнению с началом года. Согласно данным из аналитического отчета об актуальных киберугрозах компании «Positive Technologies» количество новых для 2023 г. уязвимостей за второй квартал составило более 7,5 тыс.[1].

Эксплуатацию этих уязвимостей на объектах КИИ в ходе проведения компьютерной атаки можно представить как процесс взаимодействия сложных программно-технических систем. Прогнозирование развития таких систем применительно к создаваемым системам обеспечения информационной безопасности с учетом появления новых уязвимостей программного обеспечения является достаточно сложной задачей [1]. При этом одним из важнейших аспектов прогноза состояния защищенности является прогнозирование свойств новых уязвимостей программного обеспечения.

Проблематика прогнозирования свойств новых уязвимостей программного обеспечения привлекает внимание исследователей уже достаточно давно. Однако эффективность прогнозов, полученных с помощью методов экспоненциального сглаживания [2, 3], статистических методов (Кростона, ARIMA) [4] , кластерного анализа [5], экспертных систем [6] и машинного обучения [7] оказалась не достаточной, так как результаты прогнозов существенно расходятся с реальными данными. Лингвистические

[1]Актуальные киберугрозы: II квартал 2023 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 08.04.2024).

методы Big Data, использующие информацию из специализированных форумов и конференций, где активно обсуждаются разрабатываемые и/или уже известные способы проведения компьютерных атак, с целью их прогнозирования по частоте их упоминаний не учитывают эмоциональную окраску этих обсуждений [2, 8].

В [9] рассматривается подход к вероятностному прогнозированию появления новых уязвимостей в предположении, что случайное число уязвимостей, обнаруженных в конкретном компоненте информационной автоматизированной системы в течение фиксированного периода времени, распределено по закону Пуассона. Однако это противоречит тому, что интервалы времени обнаружения новых уязвимостей не являются фиксированными и их средние значения значительно сокращаются в последние годы. По этой причине известные подходы [10] к прогнозированию будущих значений временного ряда по его текущим и прошлым значениям не могут быть применены для данного исследования.

В [11] авторами только анонсируется попытка анализа и прогнозирования динамики появления уязвимостей на основе математических методов обработки временных рядов, на основе данных из американской национальной базы данных уязвимостей National Vulnerability Database, NVD.

Альтернативой строгим математическим методам является использование искусственных нейронных сетей [7, 12], что считается привлекательным вариантом, поскольку эти подходы решают проблемы доступности, нехватки данных и шума экспериментальных данных, но эти методы испытывают серьезные проблемы с ложными срабатываниями и невозможностью обобщения, что серьезно ограничивает их применимость для прогнозирования уязвимостей.

Кроме того, основным недостатком известных методов прогнозирования уязвимостей конкретного программного обеспечения является то, что при этом не анализируются стохастические параметры уязвимостей – характеристики уязвимого компонента, последствия атаки, область действия и т.д. В то же время данные параметры позволяют получить достоверный прогноз итоговой интегральной оценки уязвимости, характеризующий ее критичность по сравнению с другими, и как следствие, количественно оценивать уровень информационной безопасности систем в процессе эксплуатации [13].

В настоящее время в основе описания свойств выявленных уязвимостей лежит стандартизированная система оценки уязвимостей в информационных системах – Common Vulnerability Scoring System (CVSS)[2]. Открытость CVSS-оценок позволяет использовать их для автоматизированного прогнозирования и оценки критичности уязвимостей.

Область применения таких прогнозов достаточно обширна. Помимо лиц, эксплуатирующих значимые объекты, другими потребителями результатов прогнозов могут являться разработчики соответствующего программного обеспечения и средств защиты информации. Поскольку определение приоритетов, своевременное обнаружение атакующего в системе, точное прогнозирование его целей, а также быстрое устранение уязвимостей может сократить количество результативных компьютерных атак на защищаемые объекты, помочь предотвратить серьезный урон КИИ и избежать масштабных негативных последствий и потерь.

Сведения, представленные в различных базах данных уязвимостей, позволяют получить обширную информацию об уязвимостях программного обеспечения (ПО),

[2]Common Vulnerability Scoring System (CVSS-SIG). FIRST website. https://www.first.org/cvss (дата обращения: 08.04.2024).

которая включает в себя, например, наименование ПО, его версию, язык, на котором написан исходный код ПО, операционную систему, под управлением которой проявляется уязвимость, и другую информацию об уязвимостях ПО. Ее можно использовать для эмпирического прогнозирования угроз информационной безопасности. Однако этого не достаточно для формирования стратегий создания и развития систем безопасности, а также формирования приоритетов на стадии разработки программного обеспечения и средств защиты информации. Необходимо применение методов аналитического моделирования для определения основных параметров уязвимостей и проводимых на их основе компьютерных атак [14].

Поэтому целью работы является разработка подхода к прогнозированию свойств новых уязвимостей программного обеспечения, сочетающего достоинства статистических методов анализа данных и аналитического моделирования, т.к. получение объективных сведений о прогнозируемых свойствах уязвимостей программно-аппаратных компонентов защищаемых объектов КИИ позволит оценивать уровень безопасности КИИ с более высокой точностью.

Основная часть исследования

Основу информационного обеспечения предлагаемого подхода к прогнозированию, сочетающего достоинства статистических методов анализа данных и аналитического моделирования, составляют сведения об уязвимостях, представленные в разделе «Уязвимости» Банка данных угроз безопасности информации ФСТЭК России[3]. На момент выполнения работы данная база сведений об уязвимостях содержала более 55 тыс. записей, из которых более 37 тыс. включали оценку уязвимости в формате CVSS v3.0 вида: «AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H».

Анализ значений метрик, отражающих основные характеристики уязвимостей позволяет сделать вывод о том, что проявление основных свойств выявленных уязвимостей представляет собой многомерный случайный процесс [15]. Поскольку проявление этих свойств происходит в случайные моменты времени, значение этого свойства не зависит от предыдущих значений, то данный процесс с тем или иным приближением можно считать марковским процессом с дискретными состояниями и непрерывным временем. Выявленное количество проявлений свойств (метрик) уязвимостей в месяц приведено на рис. 1.

Значительный объем статистических данных, полученных из Банка данных угроз ФСТЭК России, позволяет проводить достоверные прогнозы появления уязвимостей для конкретных типов аппаратной платформы, версий программного обеспечения. В качестве примера рассмотрим уязвимости операционной системы Astra Linux. Для этого выберем только те записи базы сведений об уязвимостях, у которых в поле «Наименование ОС и тип аппаратной платформы» присутствует подстрока «Astra Linux». Анализ выборки этих данных показывает, что применительно к операционной системе Astra Linux Special Edition и ее компонентам выявлено около 5400 уязвимостей. В интересах прогнозирования для выборки из этих записей проведем анализ динамики изменения свойств обнаруживаемых уязвимостей как времени существования свойства, начиная с 1 января 2017 г. Например, значение метрики «Вектор атаки (AV)» выявленной 02.01.2017 уязвимости BDU:2017-01549 определено как «Сетевой (N)», а у следующей опубликованной уязвимости BDU:2021-03350, выявленной 22.01.2017, эта метрика изменяет значение на – «Локальный (L)». Следовательно, длительность актуальности

[3]БДУ – Раздел уязвимости. URL: https://bdu.fstec.ru/vuln/ (дата обращения: 08.04.2024).

(существования) свойства «Вектор атаки (AV)» – «Сетевой (N)» составляет 20 дней, а длительность существования свойства «Вектор атаки (AV)» – «Локальный (L)» составляет 3 дня, т.к. у уязвимости BDU:2020-05848, выявленной 25.01.2017 «Вектор атаки (AV)» вновь принимает значение – «Сетевой (N)».

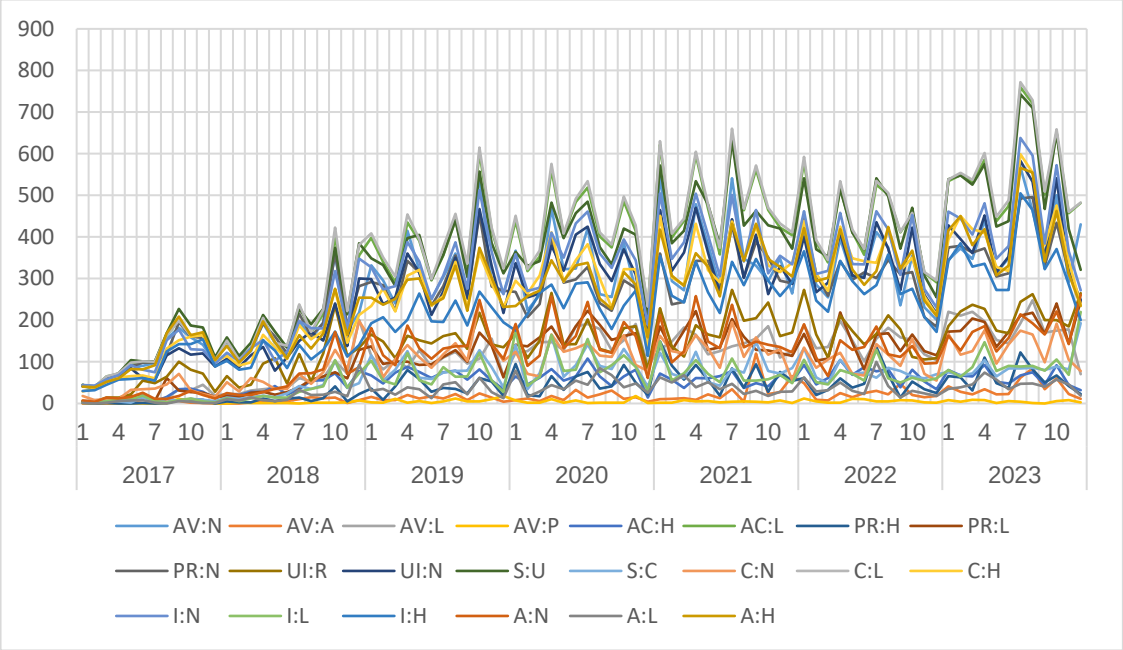


Рис. 1. Количество проявлений свойств (метрик) уязвимостей в месяц

Анализируя даты изменения значений метрик, можно вычислить длительности актуальности значений метрик при их смене и построить соответствующие временные ряды базовых метрик CVSS v3.0, а именно для следующих метрик и их значений:

1. Вектор атаки (AV): Сетевой (N), Смежная сеть (A), Локальный (L), Физический (P).
2. Сложность атаки (AC): Высокая (H), Низкая (L).
3. Уровень привилегий (PR): Высокий (H), Низкий (L), Не требуется (N).
4. Взаимодействие с пользователем (UI): Требуется (R), Не требуется (N).
5. Влияние на другие компоненты системы (S): Не оказывает (U), Оказывает (C).
6. Влияние на конфиденциальность (C): Не оказывает (N), Низкое (L), Высокое (H).
7. Влияние на целостность (I): Не оказывает (N), Низкое (L), Высокое (H).
8. Влияние на доступность (A): Не оказывает (N), Низкое (L), Высокое (H).

Как отмечалось ранее процесс существования свойств этих метрик является марковским, следовательно, имея полученные длительности актуальности значений (временные ряды актуальности метрик), можно вычислить средние значения времени актуальности свойств метрик CVSS v3.0 в течении интервала наблюдения. Так как дата выявления уязвимости в сведениях об уязвимостях Банка данных угроз безопасности информации ФСТЭК России определяется с точностью до суток, то условимся считать, что в пределах суток этот случайный процесс является однородным. Поэтому записи сведений об уязвимостях, имеющих одинаковые значения метрик CVSS v3.0 и одинаковые даты выявления считаются дублирующими, из анализируемой выборки исключаются. В тоже время не линейный рост количества выявленных уязвимостей вынуждает проводить анализ среднего времени актуальности свойств метрик до соответствующего изменения в течение определенного «окна» (интервала) анализа с относительно стационарными значениями продолжительностью в один квартал года.

В результате этого анализа получены поквартальные значения среднего времени актуальности свойств метрик до соответствующего изменения в днях. Для построения аналитических моделей от рассчитанных значений среднего времени актуальности свойств метрик до соответствующего изменения перейдем к средним значениям мгновенной интенсивности смены свойств в пределах квартала

$$\lambda(кв) = \frac{1}{\bar{t}(кв)}, \quad (1)$$

где $\lambda(кв)$ – среднее значение интенсивности для соответствующего квартала года; $\bar{t}(кв)$ – среднее время актуальности свойств метрик.

Полученные средние значения мгновенной интенсивности смены метрик $\lambda(кв)$ определяют тенденции изменений и могут быть использованы для экстраполяции соответствующего временного ряда в интересах прогнозирования значений этих интенсивностей в будущем. Для простоты расчетов прогнозирование значений интенсивностей осуществим методом регрессионного анализа, а именно методом линейной регрессии [15]. Аппроксимирующая функция зависимости среднего значения мгновенной интенсивности смены свойств соответствующей базовой метрики уязвимости от номера квартала анализа (интервала наблюдений) выявленных уязвимостей Astra Linux Special Edition, начиная с нулевого квартала (02.01.2017), имеет вид $\lambda^{рег}(кв) = a \cdot кв + b$. Полученную линейную функцию можно использовать для интерполяции при $кв \le 27$ и предсказания поведения зависимости значений интенсивностей изменения свойств метрик CVSS v3.0 от номера квартала при $кв > 27$.

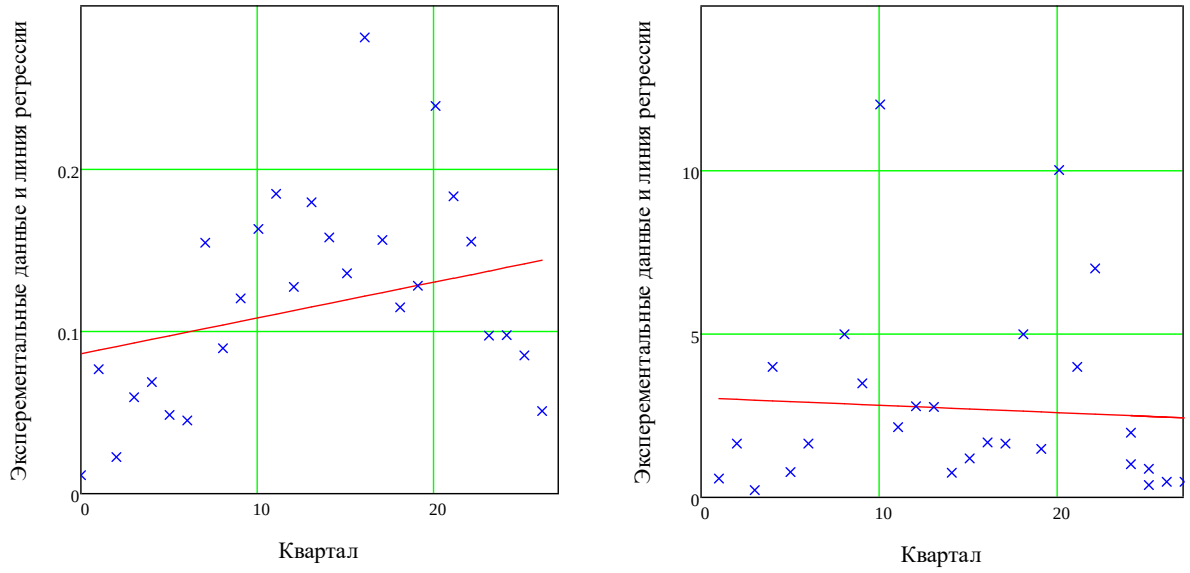
Результаты регрессионного анализа в виде коэффициентов линейной функции a, b и значений суммы квадратов абсолютных ошибок SSE приведены в табл. 1.

Графическое представление экспериментальных данных и линейной функции интенсивностей для переходов, имеющих минимальное (при смене значений метрики S:U–C) и максимальное (при смене значений метрики C:L–N) значение суммы квадратов абсолютных отклонений в зависимости от номера квартала, представлено на рис. 2 а) и б) соответственно.

Приступим к построению марковской модели для прогнозирования свойств новых уязвимостей, основанной на решении систем однородных дифференциальных уравнений Колмогорова, записанных для каждой из метрик CVSS v3.0 [16]. Процесс изменения свойств метрик CVSS v3.0 уязвимостей при их выявлении можно представить, как функционирование восьми независимых эргодических систем, находящихся в одном из 2-х, 3-х и 4-х состояниях, в зависимости от мощности множества возможных значений метрики. Графы смены состояний таких систем приведены в табл. 2.

Таблица 1. Коэффициенты линейной регрессии значений интенсивностей

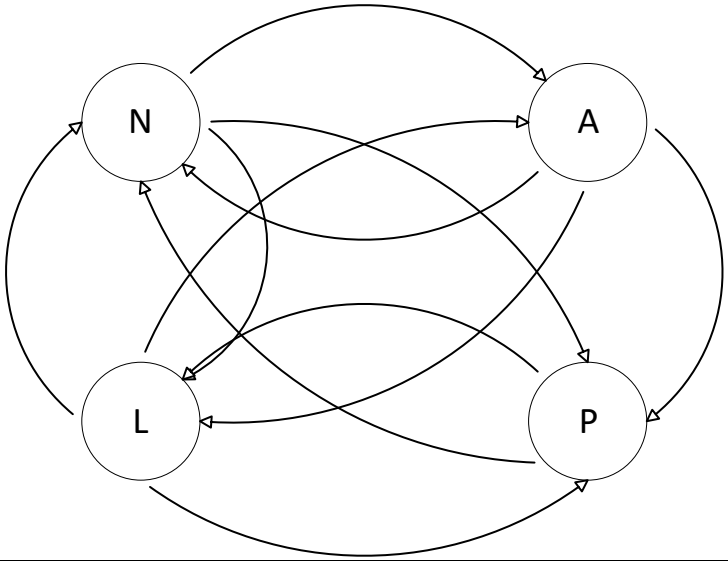
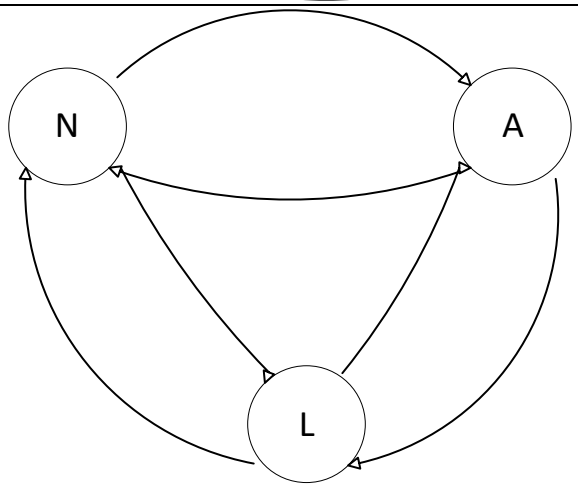
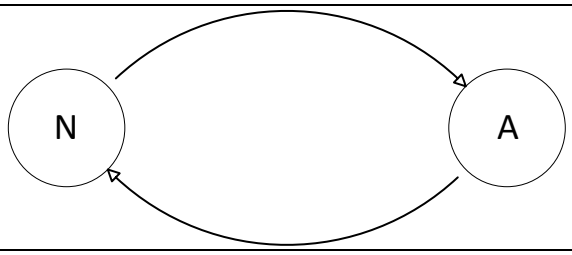
Метрика	**AV**										
Переход	**N-A**	**N-L**	**N-P**	**A-N**	**A-L**	**A-P**	**L-N**	**L-A**	**L-P**	**P-N**	**P-L**
b	0,29	0,11	0,42	1,13	1,20	1,20	1,82	1,49	1,41	1,27	1,55
a	0,02	0,02	0,01	-0,02	-0,01	-0,01	-0,04	-0,02	-0,02	-0,01	-0,03
SSE	3,15	1,12	4,58	7,76	17,47	17,47	25,05	5,35	4,16	7,32	6,93
Метрика	**AC**		**PR**			**UI**			**S**		
Переход	**H-L**	**L-H**	**H-L**	**H-N**	**L-H**	**L-N**	**N-H**	**N-L**	**R-N**	**N-R**	**U-C**
b	1,24	0,14	0,87	1,54	2,75	1,41	0,17	0,13	0,57	0,48	0,09
a	0,02	0,00	-0,02	-0,02	-0,08	-0,01	0,03	0,02	0,02	0,00	0,00
SSE	12,43	0,25	11,87	16,85	15,44	7,08	2,31	0,71	3,20	1,20	0,11
Метрика	**S**				**C**			**I**			
Переход	**C-U**	**N-L**	**N-H**	**L-N**	**L-H**	**H-N**	**H-L**	**N-L**	**N-H**	**L-N**	**L-H**
b	1,38	0,89	0,58	3,06	1,14	0,72	1,08	0,89	0,48	2,08	1,53
a	0,01	0,00	0,02	-0,02	0,06	0,01	-0,02	0,01	0,02	0,02	0,05
SSE	29,09	5,93	2,97	223,50	66,15	2,85	5,00	15,92	1,55	129,83	172,10
Метрика	**I**		**A**								
Переход	**H-N**	**H-L**	**N-L**	**N-H**	**L-N**	**L-H**	**H-N**	**H-L**			
b	0,88	1,70	1,10	1,01	2,13	2,22	0,36	0,38			
a	0,01	-0,02	0,02	0,03	-0,01	-0,01	0,01	0,01			
SSE	5,98	55,19	54,07	14,70	69,30	83,68	1,08	1,92			



а) Переход S:U–C (min SSE) *б) Переход C:L–N (max SSE)*

Рис. 2. Экспериментальные данные и линия регрессии функции интенсивностей для переходов S:U–C и C:L–N в зависимости от номера квартала

Таблица 2. Графы состояний изменения свойств метрик CVSS v3.0

Метрика	Граф состояний
AV	
PR, C, I, A	
AC, UI, S	

Для этих графов состояний (табл. 2) записаны системы уравнений Колмогорова, в каждую из которых включено нормирующее уравнение $\sum_i P_i(t) = 1$. Полученные системы уравнений приведены в табл. 3. Для эргодических систем с 3-мя и 2-мя состояниями переменные, входящие в эти уравнения отличаются только записью индексов, отождествляющих соответствующие состояния метрик CVSS v3.0.

Особенностью прогнозирования с использованием марковских моделей является наличие на временной оси зависимости моделируемого процесса двух участков: участка переходного режима и участка стационарного режима [16]. Эту особенность можно

использовать для краткосрочного прогнозирования (переходной режим) и долгосрочного прогнозирования (стационарный режим). Долгосрочное прогнозирование является предметом другого исследования.

Таблица 3. Системы дифференциальных уравнений Колмогорова

Метрика	Система уравнений Колмогорова
AV	$\frac{dP_N^{AV}(t)}{dt} = \lambda_{A-N}^{AV}(кв)\,P_A^{AV}(t) + \lambda_{L-N}^{AV}(кв)\,P_L^{AV}(t) + \lambda_{P-N}^{AV}(кв)\,P_P^{AV}(t) - $ $ - (\lambda_{N-A}^{AV}(кв) + \lambda_{N-P}^{AV}(кв) + \lambda_{N-L}^{AV}(кв))\,P_N^{AV}(t)$ $\frac{dP_P^{AV}(t)}{dt} = \lambda_{N-P}^{AV}(кв)\,P_N^{AV}(t) + \lambda_{A-P}^{AV}(кв)\,P_A^{AV}(t) + \lambda_{L-P}^{AV}(кв)\,P_L^{AV}(t) - $ $ - (\lambda_{P-N}^{AV}(кв) + \lambda_{P-L}^{AV}(кв))\,P_P^{AV}(t),$ (2) $\frac{dP_A^{AV}(t)}{dt} = \lambda_{N-A}^{AV}(кв)\,P_N^{AV}(t) + \lambda_{L-A}^{AV}(кв)\,P_L^{AV}(t) - $ $ - (\lambda_{A-N}^{AV}(кв) + \lambda_{A-P}^{AV}(кв) + \lambda_{A-L}^{AV}(кв))\,P_A^{AV}(t)$ $P_N^{AV}(t) + P_P^{AV}(t) + P_A^{AV}(t) + P_L^{AV}(t) = 1$
PR (C, I, A)	$\frac{dP_H^{PR}(t)}{dt} = \lambda_{L-H}^{PR}(кв)\,P_L^{PR}(t) + \lambda_{N-H}^{PR}(кв)\,P_N^{PR}(t) - (\lambda_{H-N}^{PR}(кв) + \lambda_{H-L}^{PR}(кв))\,P_H^{PR}(t)$ $\frac{dP_L^{PR}(t)}{dt} = \lambda_{H-L}^{PR}(кв)\,P_H^{PR}(t) + \lambda_{N-L}^{PR}(кв)\,P_N^{PR}(t) - (\lambda_{L-Y}^{PR}(кв) + \lambda_{L-N}^{PR}(кв))\,P_L^{PR}(t)$, (3) $P_H^{PR}(t) + P_L^{PR}(t) + P_N^{PR}(t) = 1$
AC (UI, S)	$\frac{dP_H^{AC}(t)}{dt} = \lambda_{L-H}^{AC}(кв)\,P_L^{AC}(t) - \lambda_{H-L}^{AC}(кв)\,P_H^{AC}(t)$, (4) $P_H^{AC}(t) + P_L^{AC}(t) = 1$

График зависимости вероятностей значений метрики «Вектор атаки (AV)» в первый квартал 2024 г. от дня с момента опубликования сведений об уязвимости при начальных условиях $P_N^{AV}(0) = 1, P_P^{AV}(0) = 0,\ P_A^{AV}(0) = 0, P_L^{AV}(0) = 0$ приведен на рис. 3. Как отмечалось выше, на временной оси зависимостей вероятностей пребывания в соответствующих состояниях наблюдаются переходные и стационарные участки. На рис. 3 видно, что в переходной период существенное значение имеют начальные условия, т.е. значения свойств метрики предыдущей опубликованной уязвимости. На стационарном участке ($t > 1.7$ дня) начальные условия уже не существенны.

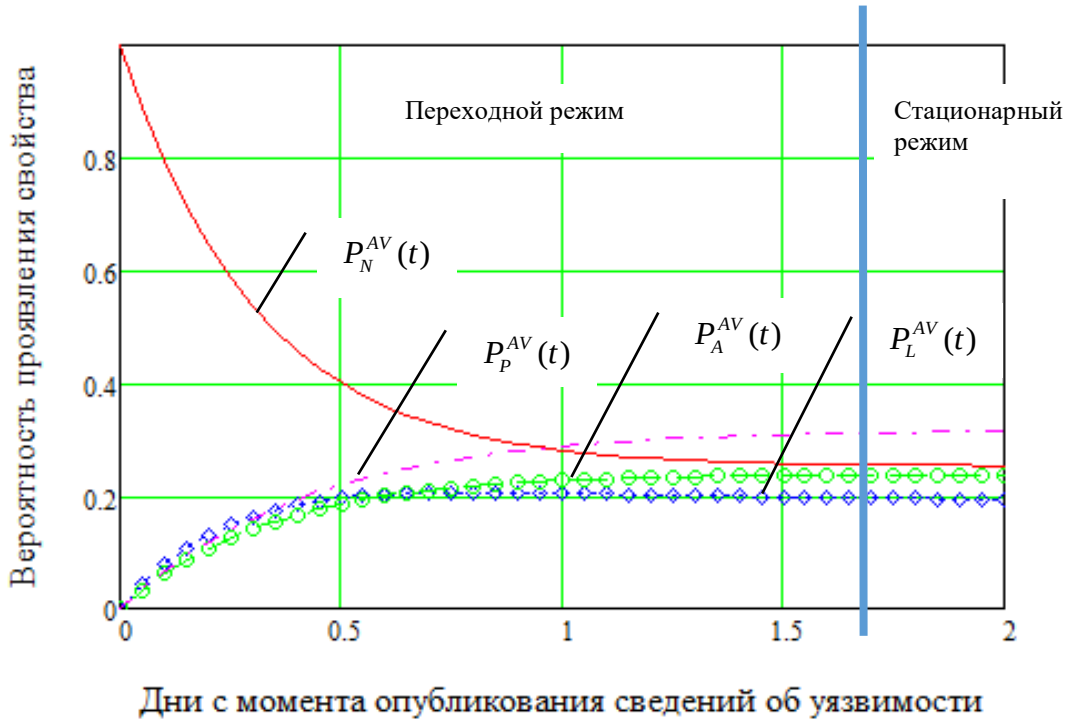


Рис. 3. График зависимости вероятностей проявления свойств метрики «Вектор атаки (AV)» от дня с момента опубликования сведений

Рассмотрим пример краткосрочного прогнозирования появления новой уязвимости операционной системы Astra Linux в течении одних суток. Зафиксируем сведения об уязвимости BDU:2023-08755, выявленной 28.11.2023. Значения метрики CVSS v3.0 определены, как «AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H». Значит, векторы начальных состояний для 8 марковских моделей будут записаны как представлено в табл. 4.

Таблица 4. Начальные значения вероятностей появления свойств метрик

№	Метрика	Начальные значения	№	Метрика	Начальные значения
1	AV	$P_N^{AV}(0)=1, P_A^{AV}(0)=0,$ $P_L^{AV}(0)=0, P_P^{AV}(0)=0$	5	S	$P_U^S(0)=1, P_C^S(0)=0$
2	AC	$P_H^{AC}(0)=0, P_L^{AC}(0)=1$	6	C	$P_H^C(0)=1, P_L^C(0)=0,\ P_N^C(0)=0$
3	PR	$P_H^{PR}(0)=0, P_L^{PR}(0)=0,\ P_N^{PR}(0)=1$	7	I	$P_H^I(0)=1, P_L^I(0)=0,\ P_N^I(0)=0$
4	UI	$P_R^{UI}(0)=1, P_N^{UI}(0)=0$	8	A	$P_H^A(0)=1, P_L^A(0)=0,\ P_N^A(0)=0$

Проведем математическое моделирование процессов проявления базовых свойств уязвимостей с использованием систем уравнений (2) – (4).

Проведенный анализ полученных зависимостей вероятностей смены значений всех метрик CVSS v3.0 показал, что в течение суток превышение значений вероятности изменения свойств происходит только для метрики «Взаимодействие с пользователем (UI)» со значения «Требуется (R)» на «Не требуется (N)». График полученной зависимости от времени с момента опубликования сведений об уязвимости приведен на рис. 4. Смену значений метрики «Взаимодействие с пользователем (UI)» подтверждает

вектор значений метрик CVSS v3.0 у уязвимости BDU:2023-08264, опубликованной на следующий день после выявления уязвимости BDU:2023-08755 – 29.11.2023. Значение метрики «Взаимодействие с пользователем (UI)» для этой уязвимости в векторе определено как AV:N/AC:L/PR:N/**UI:N**/S:U/C:H/I:H/A:H. Из этого видно, что в реальности значение метрики сменилось со значения «Требуется (R)» на значение «Не требуется (N)». Это совпадение подтверждает адекватность используемого подхода к прогнозированию и достоверность получаемых результатов.

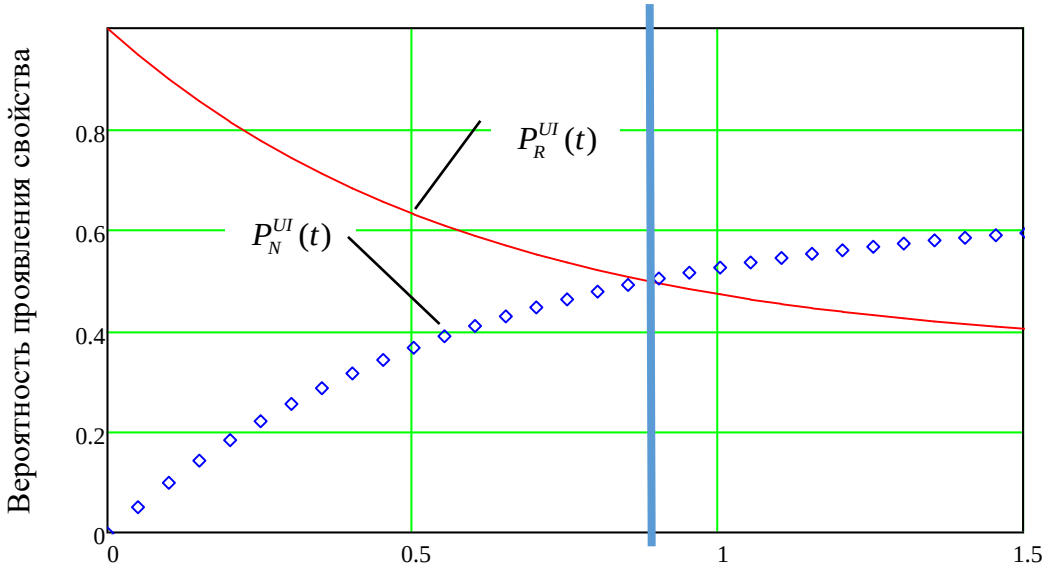


Рис. 4. Зависимость вероятностей смены значений метрики «Взаимодействие с пользователем (UI)» со значения «Требуется (R)» на «Не требуется (N)»

Заключение

Таким образом, разработан подход для краткосрочного (до одних суток) долгосрочного (до нескольких кварталов) прогнозирования свойств новых уязвимостей программного обеспечения.

Основу прогнозирования составляет представление процесса смены значений оценок метрик CVSS v3.0 уязвимостей, опубликованных как восемь независимых марковских случайных процессов с дискретными состояниями и непрерывным временем. Отличительной особенностью подхода к прогнозированию с использованием марковских моделей является описание зависимости интенсивностей смены значений метрик в виде линейной функции, зависящей от временного «окна» анализа продолжительностью в один квартал года и имеющей вид $\lambda^{рег}(кв) = a \cdot кв + b$. Полученную функцию можно использовать для интерполяции и предсказания поведения зависимости значений интенсивностей изменения свойств метрик CVSS v3.0 от номера квартала.

На примере оценок CVSS v3.0 для двух уязвимостей Astra Linux Special Edition, опубликованных последовательно друг за другом в течение суток, подтверждена адекватность используемого подхода к краткосрочному прогнозированию и достоверность получаемых результатов.

Получение объективных данных о прогнозируемых свойствах уязвимостей программно-аппаратных компонентов защищаемых объектов КИИ с использованием

разработанного подхода к прогнозированию позволит реально оценивать безопасность КИИ.

Областью применения разработанного подхода могут являться сфера разработки соответствующего программного обеспечения и средств защиты информации, а также создаваемые и эксплуатируемые системы обеспечения информационной безопасности значимых объектов КИИ Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ:

1. Саркисян С.А., Ахундов В.М., Минаев Э.С. Анализ и прогноз развития больших технических систем. М.: Наука, 1982. – 280 р.
2. Yasasin E., Prester J., Wagner G., & Schryen G. (2020). Forecasting IT security vulnerabilities - An empirical analysis. Comput. Secur., v. 88, 101610. DOI: https://doi.org/10.1016/j.cose.2019.101610.
3. Augustine M.T. and Patil D.U. A Computationally Efficient LQR based Model Predictive Control Scheme for Discrete-Time Switched Linear Systems. 60th IEEE Conference on Decision and Control (CDC), Austin, TX, USA. 2021, p. 2480–2485. DOI: 10.1109/CDC45484.2021.9683689.
4. Roumani Yaman, Joseph K. Nwankpa, Yazan F. Roumani (2015). Time series modeling of vulnerabilities. Computers & Security. V. 50, p. 32–40. DOI: https://doi.org/10.1016/j.cose.2015.03.003.
5. Movahedi Y., Cukier M., Andongabo A. and Gashi I. Cluster-Based Vulnerability Assessment Applied to Operating Systems. 13th European Dependable Computing Conference (EDCC), Geneva, Switzerland. 2017, p. 18–25. DOI: 10.1109/EDCC.2017.27.
6. Соловьев С.В., Мамута В.В. Применение экспертных методов при прогнозировании угроз безопасности информации с использованием баз данных уязвимостей. Информация и безопасность. 2014, т. 17, № 3, с. 460–463. – EDN: SZGPPP.
7. Movahedi Y., Cukier M., & Gashi I. (2019). Vulnerability prediction capability: A comparison between vulnerability discovery models and neural network models. Computers & Security. V. 87, 101596. DOI: https://doi.org/10.1016/j.cose.2019.101596.
8. Deb A., Lerman K., & Ferrara E. (2018). Predicting Cyber Events by Leveraging Hacker Sentiment Information. 9(11), 280. DOI: https://doi.org/10.3390/info9110280.
9. Кучер В.А., Агранович В.С. Использование методов теории вероятностей и математической статистики для оценки вероятностей обнаружения уязвимостей в информационных автоматизированных системах. Информационное противодействие угрозам терроризма. 2005, № 5, с. 187–191. – EDN: IBMFAD.
10. Бокс Дж. Анализ временных рядов. Прогноз и управление = Time Series Analysis. Forecasting and control: перевод с английского. Д. Бокс, Г. Дженкинс ; под ред. В. Ф. Писаренко. М.: Мир, 1974. – 197 р.
11. Калашник Е.О. Анализ и прогнозирование динамики уязвимостей. Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007, № 39, с. 94–95. – EDN: JSPVGP.
12. Сирота А.А., Вялых А.С., Вялых С.А. Прогнозирование динамики обнаружения уязвимостей программного обеспечения при помощи нейросетевых алгоритмов обработки информации. Информатика: проблемы, методология, технологии: Материалы XIII Международной научно-методической конференции, Воронеж, 07–08 февраля 2013 года. Том 3. Воронеж: Воронежский государственный университет. 2013, с. 224–228. ISBN: 978-5-9273-2015-8. URL: https://www.cs.vsu.ru/ipmt-conf/conf/2013/Программа_2013_конф_шк_v4.pdf (дата обращения: 25.04.2024).
13. Язов Ю.К., Соловьев С.В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография. СПб: Наукоемкие технологии, 2023. – 258 с.
14. Будников С.А., Бутрик Е.Е., Соловьев С.В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon. Вопросы кибербезопасности. 2021, № 6(46), с. 47–61. – EDN: XRMBZD.
15. Андронов А.М., Копытов Е.А., Гринглаз Л.Я. Теория вероятностей и математическая статистика: Учебник для вузов. СПб.: Питер, 2004. – 461 с.
16. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Высшая школа, 2000. – 383 с.

REFERENCES:

[1] Sarkisyan S.A., Akhundov V.M., Minaev E.S. Analysis and forecast of the development of large technical systems. M.: Nauka, 1982. – 280 p. (in Russian).

[2] Yasasin E., Prester J., Wagner G., & Schryen G. (2020). Forecasting IT security vulnerabilities - An empirical analysis. Comput. Secur., v. 88, 101610. DOI: https://doi.org/10.1016/j.cose.2019.101610.
[3] Augustine M.T. and Patil D.U. A Computationally Efficient LQR based Model Predictive Control Scheme for Discrete-Time Switched Linear Systems. 60th IEEE Conference on Decision and Control (CDC), Austin, TX, USA. 2021, p. 2480–2485. DOI: 10.1109/CDC45484.2021.9683689.
[4] Roumani Yaman, Joseph K. Nwankpa, Yazan F. Roumani (2015). Time series modeling of vulnerabilities. Computers & Security. V. 50, p. 32–40. DOI: https://doi.org/10.1016/j.cose.2015.03.003.
[5] Movahedi Y., Cukier M., Andongabo A. and Gashi I. Cluster-Based Vulnerability Assessment Applied to Operating Systems. 13th European Dependable Computing Conference (EDCC), Geneva, Switzerland. 2017, p. 18–25. DOI: 10.1109/EDCC.2017.27.
[6] Solovyov S.V., Mamuta V.V. Application of expert methods in predicting threats to information security using vulnerability databases. Information and Security. 2014, v. 17, no. 3, p. 460–463 (in Russian). – EDN: SZGPPP.
[7] Movahedi Y., Cukier M., & Gashi I. (2019). Vulnerability prediction capability: A comparison between vulnerability discovery models and neural network models. Computers & Security. V. 87, 101596. DOI: https://doi.org/10.1016/j.cose.2019.101596.
[8] Deb A., Lerman K., & Ferrara E. (2018). Predicting Cyber Events by Leveraging Hacker Sentiment Information. 9(11), 280. DOI: https://doi.org/10.3390/info9110280.
[9] Kucher V.A., Agranovich V.S. Using methods of probability theory and mathematical statistics to assess the probabilities of detecting vulnerabilities in automated information systems. Information counteraction to terrorist threats. 2005, no. 5, p. 187–191 (in Russian). – EDN: IBMFAD.
[10] Box J. Time series analysis. Forecast and control = Time Series Analysis. Forecasting and control: translation from English. D. Box, G. Jenkins; edited by V. F. Pisarenko. M.: Mir, 1974. – 197 p. (in Russian).
[11] Kalashnik E.O. Analysis and forecasting of the dynamics of vulnerabilities. Scientific and Technical Bulletin of the St. Petersburg State University of Information Technologies, Mechanics and Optics. 2007, no. 39, p. 94–95 (in Russian). – EDN: JSPVGP.
[12] Sirota A.A., Vyalykh A.S., Vyalykh S.A. Forecasting the dynamics of detection of software vulnerabilities using neural network algorithms for information processing. Computer science: problems, methodology, technologies: Materials of the XIII International Scientific Conference -methodological conference, Voronezh, February 07–08, 2011. Volume 3. Voronezh: Voronezh State University. 2013, p. 224–228. ISBN: 978-5-9273-2015-8. URL: https://www.cs.vsu.ru/ipmt-conf/conf/2013/Программа_2013_конф_шк_v4.pdf (accessed: 25.04.2024) (in Russian).
[13] Yazov Yu.K., Soloviev S.V. Methodology for assessing the effectiveness of information protection in information systems from unauthorized access: monograph. St. Petersburg: High technology, 2023. – 258 p. (in Russian).
[14] Budnikov S.A., Butrik E.E., Solovyov S.V. Modeling of APT-attacks exploiting the Zerologon vulnerability. Cybersecurity issues. 2021, no. 6(46), p. 47–61 (in Russian). – EDN: XRMBZD.
[15] Andronov A.M., Kopytov E.A., Gringlaz L.Ya. Probability theory and mathematical statistics: Textbook for universities. St. Petersburg: Peter, 2004. – 461 p. (in Russian).
[16] Ventzel E.S., Ovcharov L.A. Theory of random processes and its engineering applications. M.: Higher School, 2000. – 383 p. (in Russian).

Поступила в редакцию – 06 августа 2024 г. Окончательный вариант – 15 сентября 2024 г.
Received – August 06, 2024. The final version – September 15, 20224.