ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.094

DOI: 10.21822/2073-6185-2024-51-3-86-92 Оригинальная статья / Original article

Поиск оптимального пути построения системы защиты информации на основе марковских цепей

А. М. Конаков, И. И. Лившиц
Национальный исследовательский университет ИТМО,
197101, г. Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. В рамках исследования рассмотрены основные аспекты построения системы защиты информации с точки зрения оптимизации затрачиваемых ресурсов и средств на обеспечение информационной безопасности. **Метод.** В данной предметной области рассмотрены возможности структурно – параметрических моделей и марковских цепей для выявления оптимальной линии построения многоуровневой системы защиты информации. Практика показывает, что построение и внедрение многоуровневой системы защиты информации снижает для злоумышленника возможность компрометации и несанкционированного доступа к защищаемой информации. **Результат.** Проведен анализ функциональных возможностей построенных моделей, как средства поиска оптимального пути построения системы защиты информации. Проведена оценка рисков безопасности информации в наиболее уязвимых точках процессов обеспечения информационной безопасности. Разработан и предложен подход к построению многоуровневой системы защиты информации с использованием функциональных возможностей структурно – параметрических моделей и марковских цепей. Сформулирована закономерность, позволяющая определить корректность построенной системы защиты информации на основе анализа и оценки рисков безопасности информации в наиболее уязвимых точках многоуровневой системы защиты информации, в процессе перехода из одного состояния в другое. **Вывод.** Обеспечение информационной безопасности с использованием методов математического моделирования представляет собой актуальный и ценный инструмент исходя из динамичности угроз и их неопределенности в различные промежутки времени. Разработка, апробация и внедрение новых подходов на основе моделирования позволяет спрогнозировать и предотвратить наиболее вероятные действия и шаги злоумышленника, тем самым снизив уровень риска и возможного ущерба по отношению к защищаемым информационным ресурсам и системам.

Ключевые слова: информационная безопасность, математические модели, оценка рисков, моделирование процессов

Для цитирования: А.М. Конаков, И.И. Лившиц. Поиск оптимального пути построения системы защиты информации на основе марковских цепей. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(3):86-92. DOI:10.21822/2073-6185-2024-51-3-86-92

Finding the optimal way to build an information security system based on Markov chains

A.M. Konakov, I. I. Livshits
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. **Objective**. The study examined the main aspects of building an information security system from the point of view of optimizing the resources spent and funds to ensure information security. **Method.** In this subject area, the possibilities of structural-parametric models and Markov chains for identifying the optimal line for constructing a multi-level information security system are considered. Practice shows that the construction and implementation

of a multi-level information security system reduces the possibility for an attacker of compromise and unauthorized access to protected information. **Result.** An analysis of the functionality of the constructed models was carried out as a means of finding the optimal way to build an information security system. An assessment of information security risks was carried out at the most vulnerable points in the information security processes. An approach to building a multi-level information security system using the functionality of structural-parametric models and Markov chains has been developed and proposed. A pattern has been formulated that makes it possible to determine the correctness of the constructed information security system based on the analysis and assessment of information security risks at the most vulnerable points of a multi-level information security system, in the process of transition from one state to another. **Conclusion.** Ensuring information security using mathematical modeling methods is a relevant and valuable tool based on the dynamism of threats and their uncertainty at different periods of time. The development, testing and implementation of new approaches based on modeling allows us to predict and prevent the most likely actions and steps of an attacker, thereby reducing the level of risk and possible damage to protected information resources and systems.

Keywords: information security, mathematical models, risk assessment, process modeling

For citation: A.M. Konakov, I.I. Livshits. Finding the optimal way to build an information security system based on Markov chains. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(3):86-92. DOI:10.21822/2073-6185-2024-51-3-86-92

Введение. Постоянное и непрерывное развитие технологий в современном цифровом мире, неразрывно связано с увеличением угроз в информационном пространстве.

Информация становится все более ценным активом [1], а защита данных и соблюдение мер конфиденциальности становится критически важным аспектом для компаний, частных лиц и общества в целом [2,3].

Постановка задачи. В связи с этим, возрастает потребность в построении и внедрении эффективных систем защиты информации, которые позволяют обеспечить:

1. Качественную оценку рисков и угроз безопасности информации;
2. Прогнозирование и предотвращение (в некоторых случаях – заблаговременное, на ранних этапах) угроз со стороны злоумышленников;
3. Необходимый, в соответствии с требованиями, уровень защиты информации;
4. Минимизацию потерь и оперативное восстановление после нанесённого ущерба.

Методы исследования. Для предотвращения негативных событий и повышения уровня безопасности предлагается использование модели, позволяющей своими функциональными возможностями оптимально спроектировать систему защиты информации, исходя из потребностей, возможностей и динамики процессов защищаемых информационно - технологических ресурсов и систем [4,5].

Предлагаемая модель представляет собой два взаимосвязанных между собой элемента:

Схема построения многоуровневой системы защиты информации в виде структурно - параметрической модели, где на каждом уровне используются различные методы и средства обеспечения информационной безопасности (административные, технические, организационные, нормативно - методические, экономические, а также в случае необходимости, компенсирующие меры) [6]. Построенная схема (рис. 1) является наглядным примером построения комплексной системы защиты информации, но не является обязательной к внедрению и эксплуатации, так как в зависимости от внешних/внутренних факторов и потребностей может видоизменяться (количество уровней эшелонированной защиты, используемые методы и средства обеспечения безопасности).

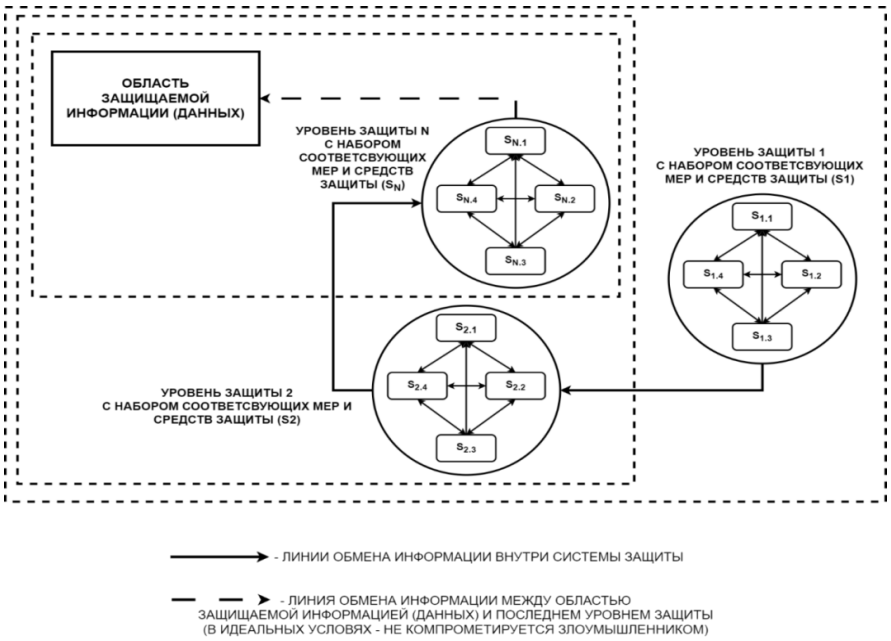

Рис. 1. Схема многоуровневой системы защиты
Fig. 1. Multi-level protection system diagram

Структурно - параметрическая модель при проектировании систем защиты информации представляют собой методологию, которая позволяет определить структуру и параметры системы защиты информации на основе анализа угроз, требований и ее функционала [7]. Такой подход обеспечивает системный подход к проектированию защиты информации, позволяя учитывать все необходимые аспекты безопасности, начиная с физической защиты объектов до применения криптографических методов защиты. Построенная модель позволяет обеспечить прозрачность и контроль состояния протекающих процессов, где на каждом уровне защиты можно корректно оценить риски и принять соответствующие меры. Также, построение общей схемы многоуровневой системы защиты информации в виде структурно – параметрической модели позволяет наглядно оценить возможности внедряемых методов и средств защиты с точки зрения их расположения и более эффективного использования.

Модель Марковской цепи. Граф состояний переходов, показан на рис. 2, где количество цепочек модели высчитывается по следующей формуле:

$$K_{э.ц.с.} = N_{ур.защ.} + 2 \quad (1)$$

Где: $\mathbf{K_{э.ц.с}}$ – количество элементов цепочки системы графа состояний переходов;

$\mathbf{N_{ур.защ}}$ – количество прогнозируемых уровней системы защиты информации

2 – числовой коэффициент, представляющий собой сумму двух областей – *«Внешняя среда»* (все, что находится за пределами информационной системы или контролируемой зоны) и *Область «*физического» и/или «цифрового» расположения защищаемых данных в информационно - технологической инфраструктуре.

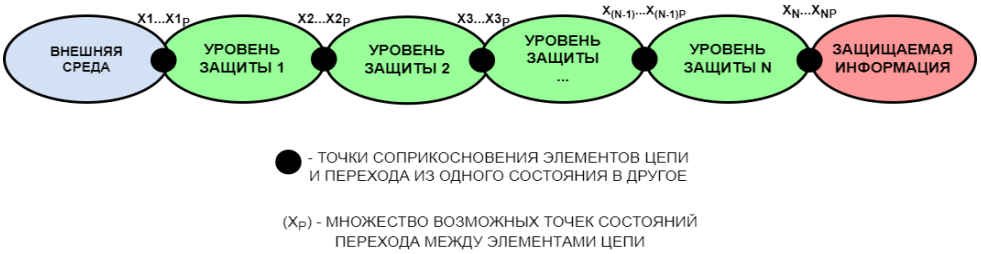

Рис. 2. Граф состояний переходов системы защиты информации
Fig. 2. Graph of transition states of the information security system

Обсуждение результатов. Следует отметить, что построение модели Марковской цепи для системы защиты информации требует точной оценки вероятностей переходов между состояниями, что может быть сложной задачей из-за факторов неопределенности

и динамичности угроз [8]. Также важно учитывать, что модель должна быть постоянно обновляться с учетом появления новых угроз и изменений в системе [9].

Модель, основанная на марковской цепи, позволяет осуществить оценку вероятности инцидентов и наиболее вероятные сценарии реализации угроз и атак, при это выполняется оценка поведения злоумышленника, позволяющая заранее предпринять необходимые меры по обеспечению безопасности.

Основная работа модели заключается в образном наложении двух вышеописанных элементов друг на друга, результат которой представляет собой «линию» оптимального и эффективного пути построения системы защиты информации исходя из анализа процессов функционирования защищаемой системы, необходимых методов и средств защиты информации с определенным набором функций (рис. 3).

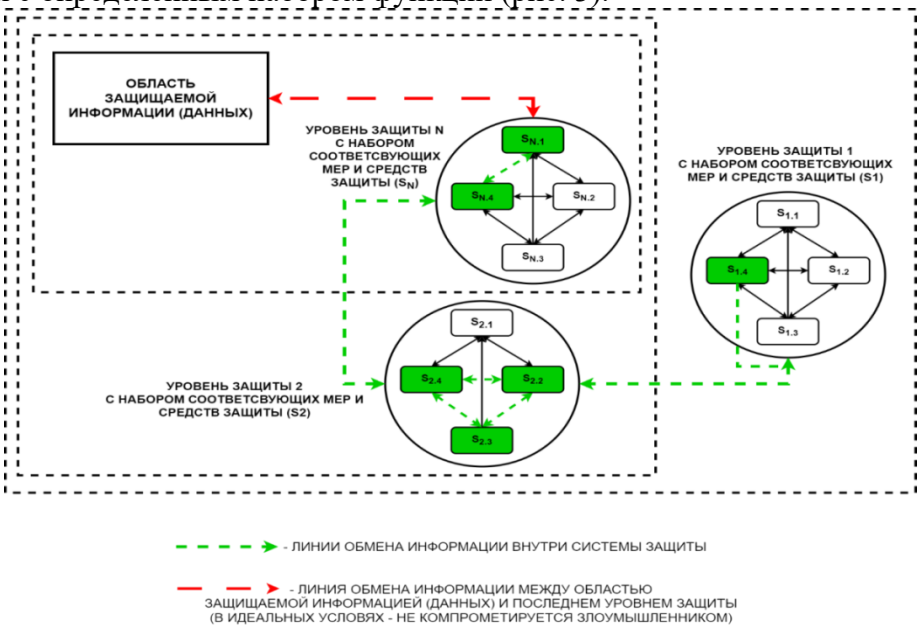

Рис. 3. Линия построения системы защиты информации
Fig. 3. Line of construction of the information security system

Отличительной особенностью предлагаемой модели является гибкая система оценки и возможность адаптации под конкретные потребности информационной системы, которые учитывают специфику вашего бизнеса, (необходимо учитывать условие непрерывности деятельности предприятия /организации, а также требований к менеджменту непрерывности деятельности [10] и обеспечения информационной безопасности [11], указанных в государственных стандартах), законодательные и нормативно - методические требования [12] с акцентом на отечественные и международные стандарты [13], а также другие факторы при разработке и внедрении системы защиты информации.

Дополнительно, на основании построенной модели состояний переходов, можно оценить риски в точках соприкосновения элементов цепи и перехода из одного состояния в другое (так как именно точки состояния перехода между уровнями защиты являются наиболее уязвимыми с точки зрения непрерывности осуществления процессов обеспечения информационной безопасности). Данный уровень риск можно рассчитать по следующей формуле

$$R_{Xp} = P_{Xp} * P_v * S_{Xp} \quad (2)$$

Где: R_{Xp} – уровень риска в точке состояния перехода;

P_{Xp} – вероятность реализации угрозы в точке состояния перехода;

P_v – вероятность наличия уязвимости в точке состояния перехода;

S_{Xp} – функциональная возможность метода/средства защиты покрывающая уязвимость в точке состояния перехода.

В табл. 1 представлены описательные характеристики принимаемых значений переменных формулы расчета уровня риска.

Таблица 1. Характеристика переменных расчета уровня риска
Table 1. Characteristics of variables for calculating the risk level

Вероятность реализации угрозы в точке состояния перехода, P_{Xp} Probability of threat realization at the point of transition state, PXp	**Вероятность наличия уязвимости в точке состояния перехода, P_v Probability of vulnerability at a transition state point, Pv**	**Функциональная возможность метода/средства защиты, SXp Functionality of the method/means of protection, SXp**		**Уровень риска в точке состояния перехода, R_{Xp} Risk level at the transition state point, RXp**	
Принимает значения в диапазоне -[0…1] Accepts values in the range -[0…1]	Принимает значения в диапазоне -[0…1] Accepts values in the range - [0…1]	3	Уязвимости покрываются частично Vulnerabilities are partially covered	[0…8)	Уровень риска минимален The risk level is minimal
		2	Покрывается больше половины уязвимостей More than half of the vulnerabilities are covered	[8…1,75)	Средний уровень риска Medium risk level
				[1.75…2,5)	Уровень риска выше среднего The risk level is above average
		1	Уязвимости покрываются полностью Vulnerabilities are fully covered	[2…3]	Максимальный уровень риска Maximum risk level

Стоит также рассмотреть следующие закономерности в представленной модели состояний переходов:

1. Если при движении в сторону области защищаемой информации (данных) в каждой последующей точке состояний переходов между уровнями защиты, уровень риска возрастает ($R_{Xp1} < R_{Xp2} < \ldots < R_{XpN}$), то система защиты информации функционирует не корректно и существует возможность несанкционированного доступа и компрометации защищаемой информации, следовательно, необходимо пересмотреть выстроенную линию защиты информации и используемых методов и средств обеспечения безопасности на каждом уровне.
2. Если при движении в сторону области защищаемой информации (данных) в каждой последующей точке состояний переходов между уровнями защиты, уровень риска снижается ($R_{Xp1} > R_{Xp2} > \ldots > R_{XpN}$), то система защиты информации корректно функционирует, и рекомендовано осуществление мониторинга состояния угроз с периодической переоценкой риска.
3. Если при движении в сторону области защищаемой информации (данных) в каждой последующей точке состояний переходов между уровнями защиты, уровень риска остается неизменным ($R_{Xp1} = R_{Xp2} = \ldots = R_{XpN}$), то система защиты информации подлежит пересмотру и/или внедрению дополнительных средств защиты с реализацией возможных компенсирующих мер.

Вывод. В статье предложена модель, с помощью которой можно осуществить построение оптимальной линии проектирования системы защиты информации информационно - технологической инфраструктуры, позволяющая отвечать современным угрозам, снижать «нагрузку» на функционирующую систему, а также обеспечивать эффективность защиты ценной информации и ресурсов в корреляции с основными положениями экономической целесообразности выделенных затрат в рамках функционирования организации [14,15].

Функциональные возможности и фундаментальные свойства Марковских цепей и структурно – параметрических моделей позволяют наглядно продемонстрировать и численно вычислить оптимальную стратегию построения системы защиты информации (оптимально подобранные методы и средства информации в зависимости от уровня защиты)

как эффективного инструмента противодействия различным видам угроз информационной среды с учётом необходимых потребностей и требований к системам защиты.

Построение системы защиты информации на основе Марковских цепей и структурно - параметрических моделей может быть сложной задачей, требующей тщательного анализа и проектирования. Оптимальный путь в данном случае будет зависеть от конкретных требований и условий системы.

Библиографический список:

1. Домбровская Л. А., Яковлева Н. А., Стахно Р. Е. Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование. – 2016. – №. 4 (22). – С. 16-19.
2. Пономарев К. Г., Кошелев С. О. Построение системы защиты информации для государственной информационной системы // Современные технологии: актуальные вопросы, достижения и инновации. – 2020. – С. 35-38.
3. Прокушев Я. Е., Пономаренко С. В., Шишов Н. В. Моделирование процессов проектирования систем защиты информации в критических информационных инфраструктурах // Computational nanotechnology. – 2022. – Т. 9. – №. 2. – С. 45-55.
4. Моделирование процессов и систем защиты информации [Текст] : учебное пособие / Е. В. Стельмашонок, В. Л. Стельмашонок ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный экономический университет", Кафедра вычислительных систем и программирования. - Санкт-Петербург : Изд-во Санкт-Петербургского гос. экономического ун-та, 2017. - 75 с.
5. Овчинников А. И. и др. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник Московского государственного технического университета им. НЭ Баумана. Серия «Приборостроение». – 2007. – №. 3. – С. 115-121.
6. Липатников В. А., Парфиров В. А. Структурно-параметрический метод защиты информационно-телекоммуникационной сети специального назначения в условиях информационного конфликта // Системы управления, связи и безопасности. – 2023. – №. 4. – С. 105-156.
7. Меньших В. В., Чиркова Н. Е. Построение структурно-параметрической модели гетерогенной системы обеспечения безопасности с использованием теории метаграфов // Вестник Воронежского института МВД России. – 2021. – №. 1. – С. 54-61.
8. Касенов А. А. и др. Марковская модель оптимизации средств защиты информации // Динамика систем, механизмов и машин. – 2019. – Т. 7. – №. 4. – С. 77-84.
9. Щеглов К. А., Щеглов А. Ю. Марковские модели угрозы безопасности информационной системы // Известия высших учебных заведений. Приборостроение. – 2015. – Т. 58. – №. 12. – С. 957-965.
10. ГОСТ Р ИСО 22301-2021 Надежность в технике. Системы менеджмента непрерывности деятельности. Требования.
11. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
12. Соловьев С. В. и др. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах //Вопросы кибербезопасности. – 2023. – №. 1. – С. 41-57.
13. Макарова Д. Г., Старикова А. А., Таратынова У. В. Построение системы защиты информации государственной информационной системы с применением международных стандартов // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 226-230.
14. Кожарский Ю. А., Масеев Д. Д. Особенности построения системы обеспечения информационной безопасности на предприятии // National Science. – 2023. – Т. 1. – №. 6. – С. 25-32.
15. Моделирование процессов и систем защиты информации. AnyLogic [Текст]: учебное пособие / А. В. Шабурова, В. А. Селифанов, В. В. Селифанов, П. А. Звягинцева, Ю. А. Исаева, А. С. Голдобина, А. В. Селифанов. – Новосибирск : СГУГиТ, 2020 – 70 с.

References:

1. Dombrovskaya L. A., Yakovleva N. A., Stakhno R. E. Modern approaches to information protection, methods, means and tools of protection. *Science, technology and education*. 2016; 4 (22):16-19. (In Russ)
2. Ponomarev K. G., Koshelev S. O. Construction of an information security system for the state information system. *Modern technologies: current issues, achievements and innovations*. 2020;35-38. (In Russ)
3. Prokushev Ya. E., Ponomarenko S. V., Shishov N. V. Modeling processes for designing information security systems in critical information infrastructures. *Computational nanotechnology*. 2022;9(2): 45-55. (In Russ)
4. Modeling processes and information security systems [Text]: textbook / E. V. Stelmashonok, V. L. Stelmashonok; Ministry of Education and Science of the Russian Federation, Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State Economic University", Department of Computer Systems and Programming. - St. Petersburg: Publishing house of the St. Petersburg State. Economic University, 2017; 75. (In Russ)

5. Ovchinnikov A.I. et al. Mathematical model of the optimal choice of means of protection against threats to the security of an enterprise computer network. *Bulletin of the Moscow State Technical University. NE Bauman. Series "Instrument making".* 2007;3:115-121. (In Russ)
6. Lipatnikov V. A., Parfirov V. A. Structural-parametric method of protecting a special-purpose information and telecommunication network in conditions of information conflict. *Control, communication and security systems.* 2023;4:105-156. (In Russ)
7. Menshikh V.V., Chirkova N.E. Construction of a structural-parametric model of a heterogeneous security system using metagraph theory. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2021; 1: 54-61. (In Russ)
8. Kasenov A. A. et al. Markov model for optimizing information security tools. *Dynamics of systems, mechanisms and machines.* 2019;7(4): 77-84. (In Russ)
9. Shcheglov K. A., Shcheglov A. Yu. Markov models of threats to the security of an information system. *News of higher educational institutions. Instrumentation*. 2015; 58(12): 957-965. (In Russ)
10. GOST R ISO 22301-2021 Reliability in technology. Business continuity management systems. Requirements. (In Russ)
11. GOST R ISO/IEC 27001-2021 Information technology. Methods and means of ensuring security. Information security management systems. Requirements; (In Russ)
12. Solovyov S.V. et al. State and prospects for the development of methodological support for technical information protection in information systems. *Issues of cybersecurity*. 2023; 1: 41-57. (In Russ)
13. Makarova D. G., Starikova A. A., Taratynova U. V. Construction of an information protection system for the state information system using international standards. *Interexpo Geo-Siberia*. 2017; 8: 226-230. (In Russ)
14. Kozharsky Yu. A., Maseev D. D. Features of constructing a system for ensuring information security at an enterprise. *National Science*. 2023;1(6): 25-32. (In Russ)
15. Modeling of information security processes and systems. AnyLogic [Text]: tutorial / A. V. Shaburova, V. A. Selifanov, V. V. Selifanov, P. A. Zvyagintseva, Yu. A. Isaeva, A. S. Goldobina, A. V. Selifanov. – Novosibirsk: SGUGiT, 2020;70. (In Russ)

Сведения об авторах:
Конаков Александр Михайлович, магистрант, helium1937@yandex.ru.
Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru
Information about authors:
Alexander M. Konakov, Master's student, helium1937@yandex.ru
Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/ Received 21.03.2024.
Одобрена после рецензирования/ Reviced 22.04.2024.
Принята в печать/ Accepted for publication 22.04.2024.