УДК 004.056.5(075.8) З-187
DOI: 10.26102/2310-6018/2022.39.4.005

# Модель функционирования защищаемой корпоративной информационной системы

**А.В. Попов[1]✉, О.Н. Чопоров[2], Ю.П. Преображенский[3]**

*[1]Воронежский государственный технический университет, Воронеж, Российская Федерация*
*[2]Воронежский государственный медицинский университет, Воронеж, Российская Федерация*
*[3]Воронежский институт высоких технологий, Воронеж, Российская Федерация*
*otdelaaa@gmail.com✉*

***Резюме.*** В России в рамках реализации Указа Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации (РФ) на период до 2024 года» входит направление по обеспечению информационной безопасности (ИБ) в области государственной и общественной безопасности РФ, сформулированное как «повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации». В работе предложена математическая модель телекоммуникационного трафика на основе набора фрактальных параметров и его фазового портрета, позволяющая более эффективно, чем только по значениям показателя Херста и корреляционной размерности оценивать наличие и отсутствие сетевых атак. Предложенная в работе модель включает в себя марковскую модель по защите корпоративной информационной системы, что дает большое преимущество в определении вида информационной угрозы и ее эффективной ликвидации. Для проверки модели на эффективность применяется система интегральных показателей с учетом времени нахождения системы во всех состояниях. Данная модель может применяться для любых организаций с корпоративно-информационной системой, т. к. определяет среди огромной массы угроз, лишь те, которые представляют опасность именно для корпоративной системы.

***Ключевые слова:*** информационная безопасность, корпоративная система, алгоритм, модель, информационные угрозы.

***Для цитирования:*** Попов А.В., Чопоров О.Н., Преображенский Ю.П. Модель функционирования защищаемой корпоративной информационной системы. *Моделирование, оптимизация и информационные технологии*. 2022;10(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1155 DOI: 10.26102/2310-6018/2022.39.4.005

# Functional model of the protected corporate information system

**A.V. Popov[1]✉, O.N. Choporov[2], Y.P. Preobrazhenskiy[3]**

*[1]Voronezh State Technical University, Voronezh, Russian Federation*
*[2]Voronezh State Medical University, Voronezh, Russian Federation*
*[3]Voronezh Institute of High Technologies, Voronezh, Russian Federation*
*otdelaaa@gmail.com✉*

***Abstract.*** The Decree of the President of the Russian Federation No. 204, dated 07.05.2018, "On national goals and strategic objectives of the development of the Russian Federation (RF) for the period until

 

2024" defines the direction of ensuring information security (IS) in the field of state and public security of the Russian Federation as "improving the security of the functioning of information infrastructure facilities with a view to ensuring sustainable interaction of state bodies, preventing foreign control over the functioning of such facilities, ensuring the integrity, stability and security of the unified telecommunication network of the Russian Federation as well as ensuring the security of information transmitted through it and processed in information systems on the territory of the Russian Federation." The paper proposes a mathematical model of telecommunication traffic based on a set of fractal parameters and its phase portrait, which helps to evaluate the presence and absence of network attacks more efficiently than solely by the values of the Hurst index and the correlation dimension. The model suggested in the paper includes a Markov model for protecting a corporate information system, which gives a great advantage in determining the type of information threat and its effective elimination. To test the efficiency of the model, a system of integral indicators is employed with consideration to the time spent by the system in all states. The model is suitable for all organizations using corporate information systems because it identifies only those threats that are dangerous to the enterprise system.

***Keywords:*** information security, corporate system, algorithm, model, information threats.

***For citation:*** Popov A.V., Choporov O.N., Preobrazhenskiy Y.P. Functional model of the protected corporate information system. *Modeling, Optimization and Information Technology*. 2022;10(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1155 DOI: 10.26102/2310-6018/2022.39.4.005 (In Russ.).

## Введение

Актуальность исследования определяется необходимостью эффективного и результативного противодействия компьютерным атакам в корпоративных информационных системах, масштаб и сложность которых постоянно растет при совершенствовании способов реализации с учетом развития информационно-коммуникационных технологий, когда при применении традиционных стратегий и систем обеспечения ИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, невозможно обеспечить требуемый уровень ИБ организации.

Проведенный анализ показывает необходимость исследования и разработки научно обоснованной модели и принципов построения организационно-технических средств обеспечения ИБ для корпоративных информационных систем.

Целью работы является разработка модели функционирования защиты корпоративной информационной системы.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ существующих подходов защиты корпоративной информационной системы.
2. Разработать модель работы корпоративной информационной системы.
3. Разработать модель защиты корпоративной информационной системы.

## Материалы и методы

Начальная информация относительно предложенного способа определяется математической моделью, которая представляет процесс работы защищаемого объекта. В основном, работу КИС, если предполагается какая-либо угроза и есть метод, позволяющий ее найти и ликвидировать, можно формализовать структурной схемой, которая показана на Рисунке 1.

Все описанные состояния отличаются друг от друга условиями работы системы в указанное время.

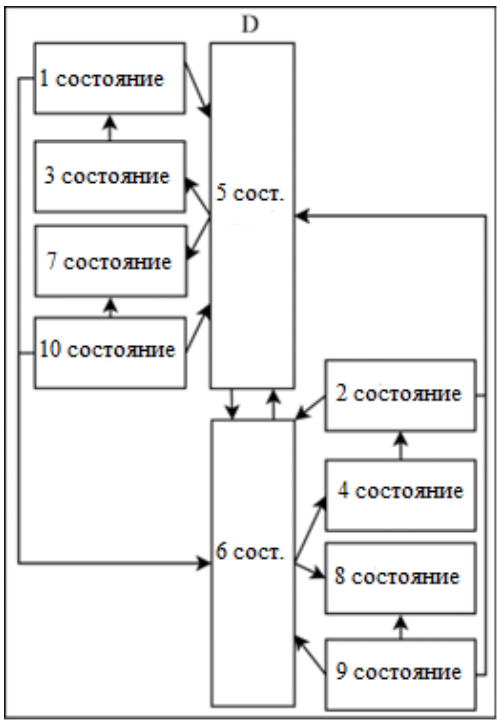


Рисунок 1 – Структурная схема функционирования защищаемой КИС
Figure 1 – Block diagram of the protected corporate information system

Вершинами в данной схеме описывается, в каком состоянии находится процесс функционирования, а при помощи стрелок представляется процесс перехода от одного состояния к другому [1]. Существует десять основных состояний $(a_1 - a_{10})$ представленного процесса, показанного на Рисунке 2.

Представленный список системных состояний представляет собой полную группу событий. Осуществление переходов от одного состояния к другому, что представлено Рисунком 4, будет определяться характерностью происходящих процессов, которые подвергаются анализу [8].

Осуществление переходов $a_5 \to a_6$, $a_6 \to a_5$ проводится, когда правонарушители активизируют или же ослабляют свою деятельность, если система меняет свою конфигурацию, меняются ее контрагенты, или же если меняются прочие условия работы системы. Если данные условия будут меняться, то это значительно повлияет на актуализацию или неактуальность угрожающих ситуаций.

Осуществление переходов $a_5 \to a_3$, $a_5 \to a_7$ производится при ситуации, если системой применяются защитные средства, при помощи которых находятся угрозы. Переход $a_5 \to a_3$ будет обозначать, что угроза успешно была обнаружена.

Осуществление перехода $a_5 \to a_7$, говорит о том, что угроза была пропущена, когда применялись защитные средства. Осуществление перехода $a_3 \to a_1$ производится при ликвидации найденной угрозы, а переход $S_7 \to S_9$ – когда неверные данные о возникновении угрозы выдаются за действительные.

Переходы $a_6 \to a_4$, $a_6 \to a_8$, $a_4 \to a_2$, $a_8 \to a_{10}$ будут соответствовать ситуациям, при которых нет данных угроз. Однако вместе с этим, защитные средства способны создавать сигналы об угрозах, являющихся ложными.


Рисунок 2 – Виды состояний при работе КИС
Figure 2 – State views in corporate information systems

## Результаты

Учитывая центральную предельную теорему, описанную теорией вероятности относительно различных событий, описание графа, представленного на Рисунке 4, можно произвести математическим аппаратом, описывающим Марковские процессы [7]. С помощью данного аппарата представление модели процессов, которые подвергаются анализу, осуществляется системой линейных дифференциальных уравнений [2]. При этом, при помощи этих сигналов защитные мероприятия могут срабатывать неадекватно, и это показывает переход $a_8 \to a_{10}$. Проведение перехода $a_4 \to a_2$ осуществляется в случае корректного определения защитной системой отсутствия угрожающих ситуаций без применения каких-либо дополнительных мероприятий по защите. Представленная модель основывается при своей работе на логике, описанной далее.

На наиболее верхнем уровне систему можно представить исключительно в виде 2-х состояний, обозначающих отсутствие указанных угроз (состояния 2, 4, 6, 8, 10), или же их наличие (состояния 1, 3, 5, 7, 9). Данные состояния делятся еще на 2 состояния, характеризуемые наличием или отсутствием средств, с помощью которых находится угроза. В итоге формируется четыре различных состояния (Рисунок 5 В). Состояния 1, 3, 7 и 9, говорят о том, что угроза присутствует, если применяются средства защиты, при других данные средства не применяются.

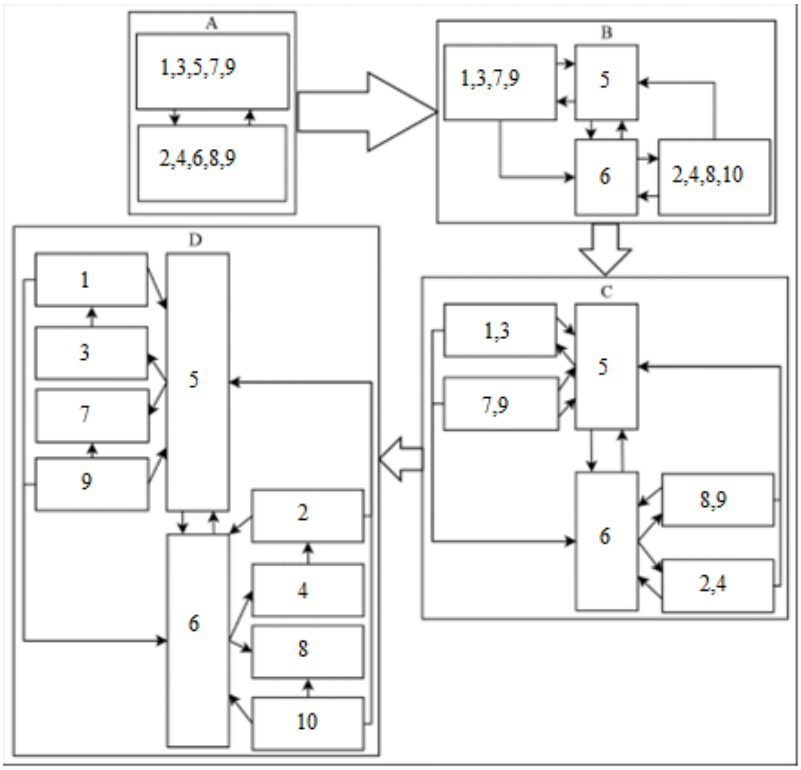


Рисунок 3 – Формирование модели работы корпоративной информационной системы
Figure 3 – Development of the model of corporate information system operation

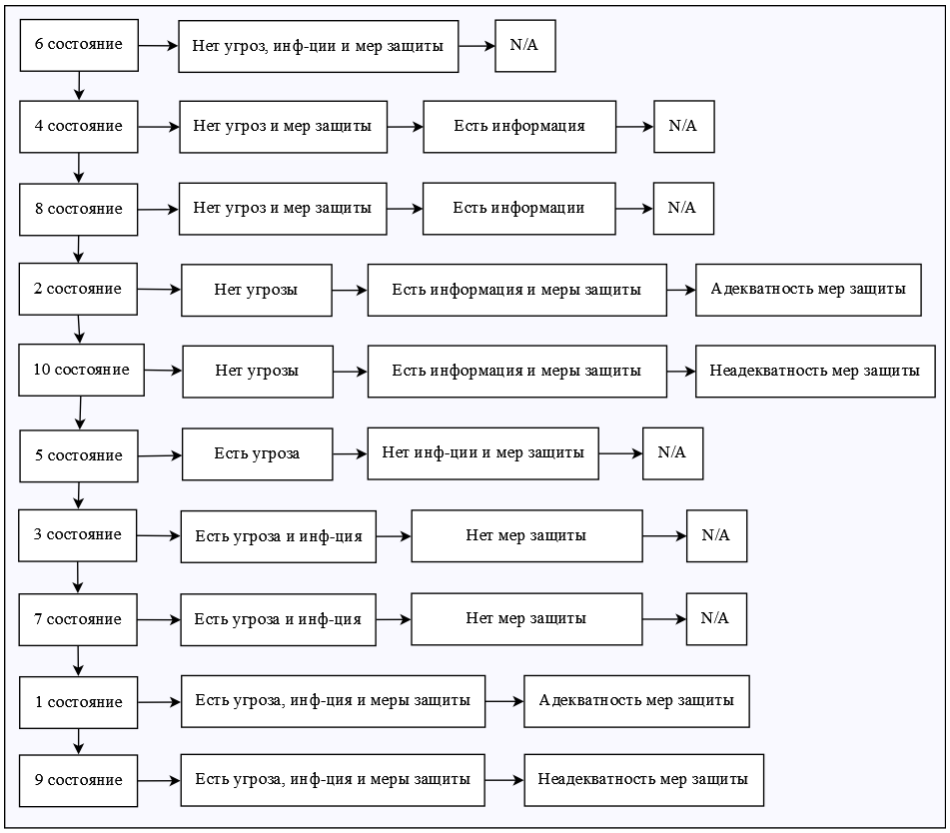


Рисунок 4 – Классифицирование состояний
Figure 4 –State classifying

Прочие состояния свидетельствуют о работе системы, когда угроз нет, когда применяются защитные средства (состояния 2, 4, 8, 10) и когда они не применяются (состояние 6). Любое из состояний, описывающее функционирование системы, когда применяются средства, помогающие найти угрозу, делятся на 2 отдельных состояния, определяющие, насколько результативным был поиск угроз (Рисунок 5 С). Соответственно при состоянии системы 3, а также 7, это будет означать, что угроза была найдена или же нет.

При состояниях 4 или 8 проводится правильная оценка ситуации на то, что угрозы нет, и возникновение ложной тревоги. После состояний 3, 7, 4, а также 8, система меняется на состояния 1, 9, 2 и 10, обозначающие включение защиты после того как угроза была найдена. Представленному ранее графу будет соответствовать система, в которой находятся линейные дифференциальные уравнения в количестве десяти штук.

Любое из них будет производить описание зависимости того, в каком из положений будет находиться система - $a_1 ... a_{10}$ от временного фактора [14]:

$$
\begin{aligned}
&\frac{dP(t)}{dt} = \lambda_{31}P_3(t) - (\lambda_{15} + \lambda_{16})P_1(t)\\
&\frac{dP_2(t)}{dt} = \lambda_{42}P_4(t) - (\lambda_{25} + \lambda_{26})P_2(t)\\
&\frac{dP_3(t)}{dt} = \lambda_{53}P_5(t) - \lambda_{31}P_3(t)\\
&\frac{dP_4(t)}{dt} = \lambda_{64}P_6(t) - \lambda_{42}P_4(t)\\
&\frac{dP_5(t)}{dt} = \lambda_{15}P_1(t) + \lambda_{25}P_2(t) + \lambda_{65}P_6(t) + \lambda_{95}P_9(t) - (\lambda_{53} + \lambda_{56} + \lambda_{57})P_5(t)\\
&\frac{dP_6(t)}{dt} = \lambda_{16}P_1(t) + \lambda_{26}P_2(t) + \lambda_{56}P_5(t) + \lambda_{96}P_9(t) + \lambda_{10,6}P_{10}(t) - (\lambda_{64} + \lambda_{65} + \lambda_{68})P_6(t)\\
&\frac{dP_7(t)}{dt} = \lambda_{57}P_5(t) - \lambda_{79}P_7(t)\\
&\frac{dP_8(t)}{dt} = \lambda_{79}P_7(t) - (\lambda_{95} + \lambda_{96})P_9(t)\\
&\frac{dP_9(t)}{dt} = \lambda_{64}P_6(t) - \lambda_{42}P_4(t)\\
&\frac{dP_{10}(t)}{dt} = \lambda_{8,10}P_8(t) - (\lambda_{10,5} + \lambda_{10,6})P_{10}(t)
\end{aligned}
\qquad (1)
$$

Результатом данной работы является проведение эксперимента по представленной выше методике. При проведении эксперимента важно рассмотреть различные ситуации при захвате трафика:

1. В течение всего времени захвата трафика DDoS-атака не происходила (нормальный режим).

2. В течение части временного интервала сетевой атаки не было, а в другой части временного интервала происходила DDoS-атака.

3. В течение всего времени захвата трафика происходила DDoS-атака.

Схема проведения эксперимента представлена на Рисунках 5 и 6, где на Рисунке 5 представлен захват трафика при моделировании нормальной работы корпоративной сети компании (состояние 1), а на Рисунке 6 представлен захват трафика при моделировании

DDoS-атаки, путем увеличения трафика второго севера и подключения третьего сервера для увеличения количества запросов к серверу один (состояние 2 и 3).

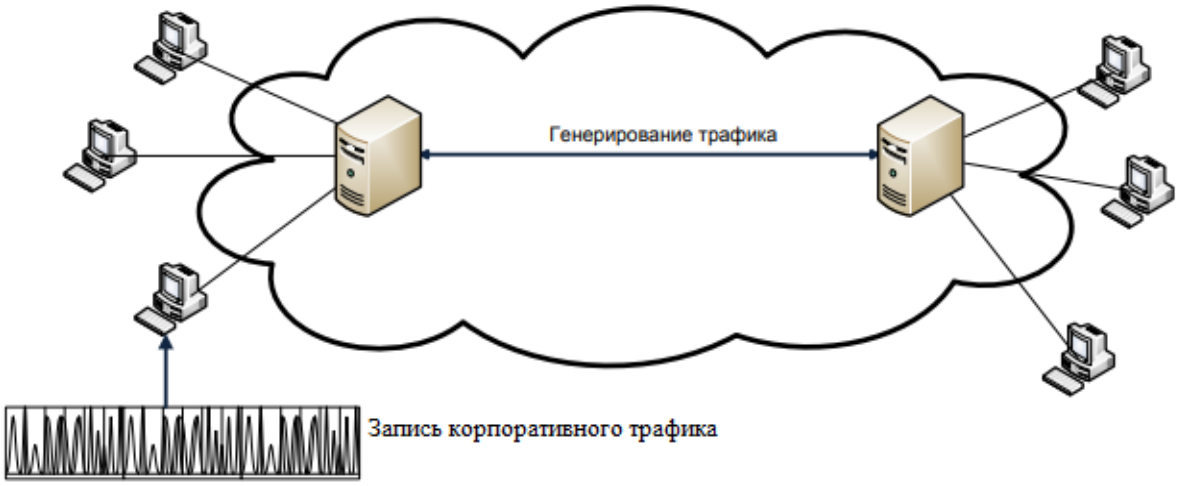


Рисунок 5 – Эксперимент моделирования нормальной работы сети
Figure 6 – Experiment on modeling the normal performance of a network

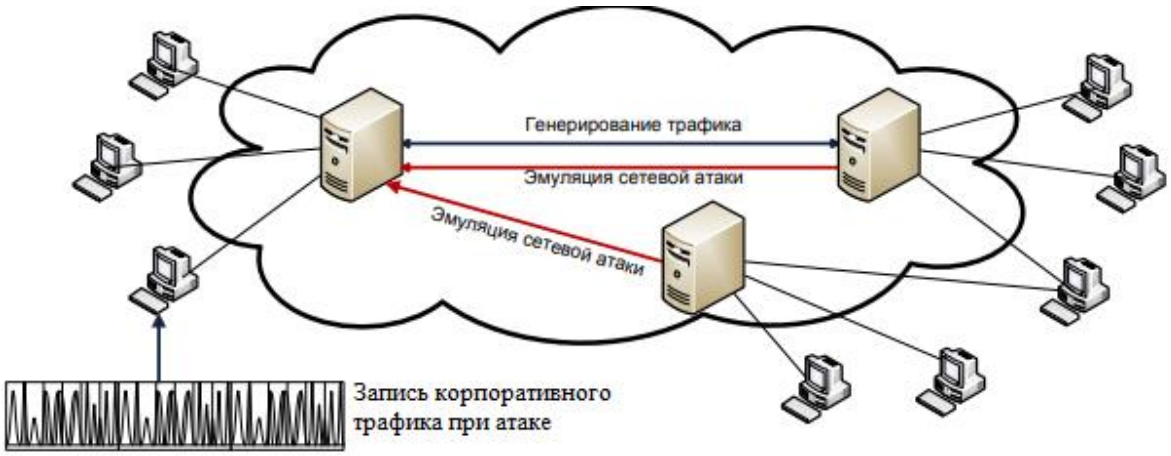


Рисунок 6 – Эксперимент при моделировании DDoS-атаки
Figure 6 – Experiment on modeling a DDos attack

Для анализа использовались временные ряды с числом выборок не менее 20000 значений. Это позволяет проводить расчет фрактальных мер и построение фазового портрета системы в течение 2-3 минут. В работе было исследовано 12 захваченных трафиков на сетях оператора связи в нормальном устойчивом состоянии и 2 трафика во время проведения сетевой атаки.

## Обсуждения

В данной системе $P_1(t),...,P_{10}(t)$ являются вероятностями того, что система будет находиться в каком-либо из состояний от 1 до 10 во время t. $\lambda_{ij}$ определяет, насколько интенсивным будет переход от состояния i до состояния j. Величина значений $\lambda_{ij}$ будет зависеть от того, какая применяется программа защиты $PRG_k$.

Стоит заметить, что когда решается определенная система уравнений, выводится вероятность, которая представляет, как будет вести себя система, если присутствует определенная угроза при применении какой-либо из защитных программ $PRG_k$.

Но здесь для более простого понимания формы, в которой показана зависимость вероятностей от уравнительных коэффициентов $PRG_k$, не учитывается потеря общности. Кроме того, интенсивность $\lambda_{ij}$ перехода от одного состояния к другому рассчитывается при помощи выражения:

$$\lambda_{ij} = g_{ij} / \overline{t_{ij}}, \quad (2)$$

здесь $t_{ij}$ – значение усредненного времени перехода от состояния i к состоянию j при условиях, близких к идеальным;

$g_{ij}$ – уровень вероятности, что этот переход будет осуществлен.

В том случае, когда значения этих показателей есть, тогда решение системы дифференциальных уравнений будет довольно простым: численными способами, а также аналитически. Также при определенном виде угрозы и используемых защитных программах у модели обязаны быть собственные изначальные значения и характеристики. Если можно узнать, в каком состоянии сейчас находится система, и если известны значения $\lambda_{ij}$, то угрозы можно предсказывать. Теперь перейдем к рассмотрению алгоритма, по которому распределяются меры при обработке рисков, которые определила представленная модель (алгоритм № 4). Чтобы сгруппировать эти меры, применяется принцип, который называется «защитой в глубину» [9] (Рисунок 7).

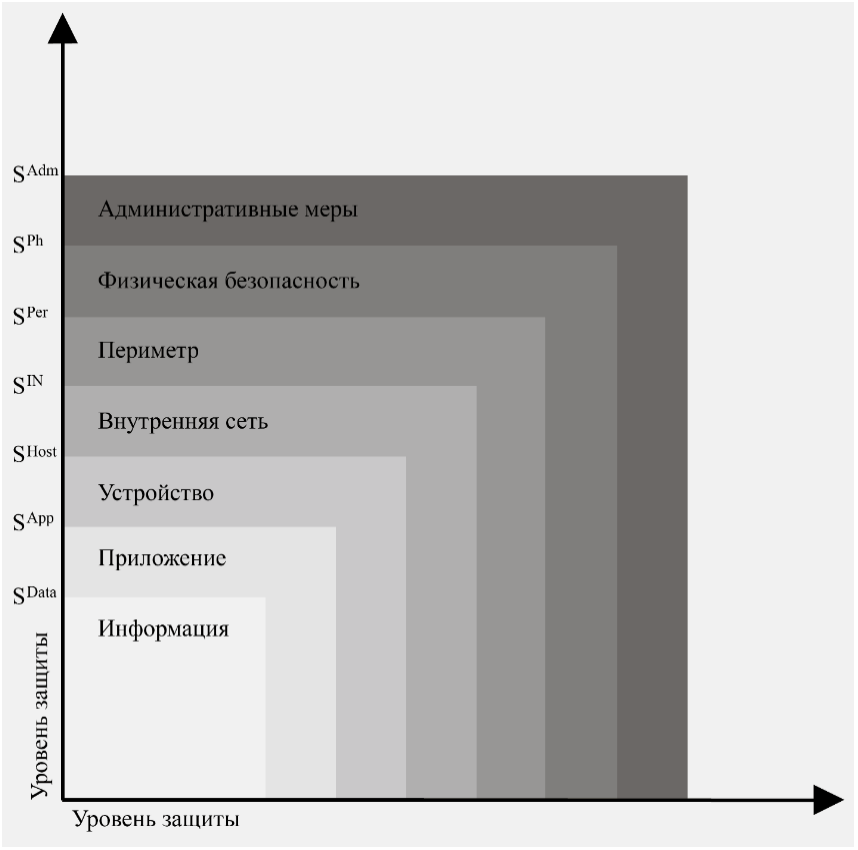


Рисунок 7 – Защитные уровни при использовании «защиты в глубину»
Figure 5 – Protective levels in operation of “defense in depth”

В соответствии с данным принципом, любая из мер, позволяющая уменьшить риски, делится по защитным уровням, относительно сфер, на которые они влияют. Меры могут быть административными, предоставлять безопасность в физическом плане – в периметре, оборудовании, внутренней сети, данных. Соответственно, все эти меры являются каким-либо защитным уровнем [3]. Чтобы применить данный принцип, ИМОРС распределяют относительно защитных уровней $t^i$ (по алгоритму № 4).

Этап № 1. Применяя модель нахождения угрозы $G_{угр}$, находим уязвимости $V^i \subseteq V$, и их можно использовать при ликвидации угроз $t^i$.

Этап № 2. Относительно угроз $t^i$, а также по всем уязвимостям $v^j \in V^i$, находим ИМОРС $S^i_{ИМОРС} \subseteq S_{ИМОРС}$, , по которым исполняется условие $L^V_S\left(v^j, s^k\right)=1$ и $L^T_S\left(t^i, s^k\right)=1$, с $s^k \in S^i_{ИМОРС}$.

Этап № 3. В соответствии с защитным уровнем, находящимся в МОР, все из элементов, относящиеся к множеству $s^k \in S^i_{ИМОРС}$, будут присвоены к какому-либо предполагаемому множеству $S^{Adm}_{OPC}, S^{Ph}_{OPC}, S^{Per}_{OPC}, S^{IN}_{OPC}, S^{Host}_{OPC}, S^{App}_{OPC}$, или же $S^{Data}_{OPC}$. Чтобы наглядно описать данный алгоритм, мы сформировали блок-схему, представленную на Рисунке 8.

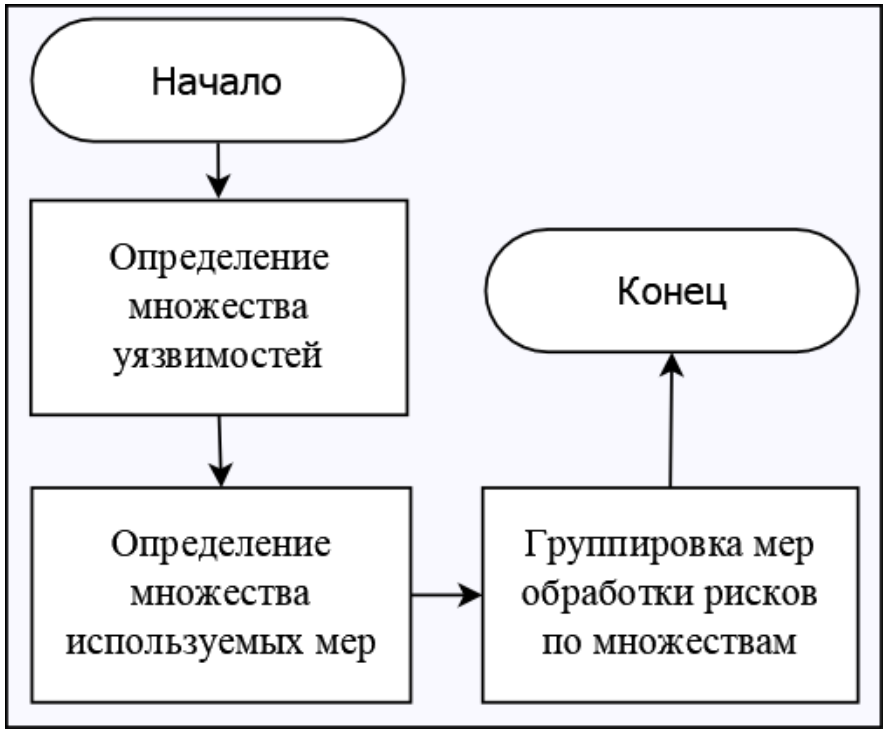


Рисунок 8 – Исполнение алгоритма № 4
Figure 8 – Implementation of algorithm No. 4

После выполнения модуля расчета фрактальных параметров и фазового пространства сохраняется изображение с фазовым портретом, который передается на обработку в модуль анализа цвета, и в результате делается вывод о наличии/отсутствии DDoS-атаки. В настоящее время интерес представляло доказательство возможности использования ряда фрактальных параметров и фазового пространства для выявления сетевых атак.

## Заключение

Была сформирована модель, позволяющая оценить, насколько эффективной является защита КИС от угроз различного типа. Данная модель в своей основе применяет марковскую модель работы защищенной корпоративной информационной системы, позволяющей осуществлять ее комплексную защиту от различных угроз информационного характера. Весь процесс работы представленной модели формализуется в состояниях, которые раньше не изучались. Эффективность работы защитных средств будет оцениваться при применении данной модели на основе интегрального показателя, определяющего эффективность работы корпоративной информационной системы, учитывая время ее нахождения во всех состояниях и достижение частной эффективности в них. Проведено создание алгоритма, с помощью которого распределяются меры по обработке рисков, а также ликвидации выявленных угроз.

## СПИСОК ИСТОЧНИКОВ


1. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Проблемы оценки характеристик пользователей в больших системах. *Вестник Воронежского института высоких технологий*. 2021;36(1):103–106.
2. Львович И.Я., Альтварг М.С., Абрамов М.И. Характеристики методов и средств управления программными проектами. *Вестник Воронежского института высоких технологий.* 2021;36(1):47–50.
3. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Проблемы анализа жизненного цикла IT-продуктов. *Вестник Воронежского института высоких технологий.* 2021;36(1):66–69.
4. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. О проблемах защиты данных в информационных системах. *Вестник Воронежского института высоких технологий.* 2021;36(1):70–73.
5. Коростелева Н.А., Батищев П.А., Денисенко С.С. Проблемы оценки эффективности работы организаций. *Вестник Воронежского института высоких технологий.* 2021;36(1):101–103.
6. Львович Э.М., Чупринская Ю.Л., Кравцова Н.Е. Особенности типологии проектных рисков. *Вестник Воронежского института высоких технологий.* 2021;37(2):104–106.
7. Львович Э.М., Чупринская Ю.Л., Кравцова Н.Е. Способы оценки и анализа проектных рисков. *Вестник Воронежского института высоких технологий.* 2021;37(2):107–109.
8. Коростелева Н.А., Попова С.С., Новичкова А.А. О проблемах моделирования функционирования организаций. *Вестник Воронежского института высоких технологий.* 2021;37(2):31–33.
9. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Об истории развития автоматизированных систем, связанных с управлением. *Вестник Воронежского института высоких технологий*.2021;37(2):75–78.
10. Львович Я.Е., Львович И.Я., Волкова Н.В. Проблемы построения корпоративных информационных систем на основе web-сервисов. *Вестник Воронежского государственного технического университета.* 2021;7(6):8–10.
11. Комаристый Д.П., Агафонов А.М., Степанчук А.П., Коркин П.С. Использование информационных систем на предприятиях. *Вестник Воронежского института высоких технологий.* 2021;21(2):104–106.

12. Гостева Н.Н., Гусев А.В. Информационные системы в управлении производством. *Вестник Воронежского института высоких технологий.* 2017;20(1):58–60.
13. Шапаев А.В., Юдаков Д.А., Часовской А.А. Проблемы поиска текстовой информации в больших объемах данных. *Вестник Воронежского института высоких технологий.* 2019;28(1):113–115.
14. Львович И.Я., Кравцова Н.Е., Чупринская Ю.Л. Особенности решений для обработки текстовых данных. *Вестник Воронежского института высоких технологий.* 2019;28(1):89–92.

## REFERENCES

1. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. Problems of assessing user characteristics in large systems. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;36(1):103–106. (In Russ.).
2. Lvovich I.Ya., Altvarg M.S., Abramov M.I. Characteristics of methods and tools for managing software projects. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;36(1):47–50. (In Russ.).
3. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. Problems of life cycle analysis of IT products. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;36(1):66–69. (In Russ.).
4. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. About the problems of data protection in information systems. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;36(1):70–73. (In Russ.).
5. Korosteleva N.A., Batishchev P.A., Denisenko S.S. Problems of evaluating the effectiveness of organizations. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;36(1):101–103. (In Russ.).
6. Lvovich E.M., Chuprinskaya Y.L., Kravtsova N.E. Features of the typology of project risks. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;37(2):104–106. (In Russ.).
7. Lvovich E.M., Chuprinskaya Y.L., Kravtsova N.E. Methods of assessment and analysis of project risks. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;37(2):107–109. (In Russ.).
8. Korosteleva N.A., Popova S.S., Novichkova A.A. On the problems of modeling the functioning of organizations. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;37(2):31–33. (In Russ.).
9. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. On the history of the development of automated systems related to management. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;37(2):75–78. (In Russ.).
10. Lvovich Ya.E., Lvovich I.Ya., Volkova N.V. Problems of building corporate information systems based on web services. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh State Technical University.* 2021;7(6):8–10. (In Russ.).
11. Komaristy D.P., Agafonov A.M., Stepanchuk A.P., Korkin P.S. The use of information systems in enterprises. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;21(2):104–106. (In Russ.).
12. Gosteva N.N., Gusev A.V. Information systems in production management. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2017;20(1):58–60. (In Russ.).

13. Shapaev A.V., Yudakov D.A., Chasovskoy A.A. Problems of searching for textual information in large volumes of data. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2019;28(1):113–115. (In Russ.).
14. Lvovich I.Ya., Kravtsova N.E., Chuprinskaya Yu.L. Features of solutions for text data processing. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2019;28(1):89–92. (In Russ.).

## ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

**Чопоров Олег Николаевич,** доктор технических наук, профессор Воронежского государственного медицинского университета, Воронеж, Российская Федерация.
*e-mail:* choporov_oleg@mail.ru
ORCID: 0000-0002-3176-499X

**Oleg Nikolaevich Choporov,** Doctor of Technical Sciences, Professor at Voronezh State Medical University, Voronezh, Russian Federation.

**Попов Андрей Вениаминович,** аспирант Воронежского государственного технического университета, кафедра систем информационной безопасности, Воронеж, Российская Федерация.
*e-mail:* otdelaaa@gmail.com

**Andrey Veniaminovich Popov**, Postgraduate Student, Voronezh State Technical University, Department of Information Security Systems, Voronezh, Russian Federation.

**Преображенский Юрий Петрович**, кандидат технических наук, доцент Воронежского института высоких технологий, Воронеж, Российская Федерация.
*e-mail:* petrov@vivt.ru

**Yuri Petrovich Preobrazhenskiy**, Candidate of Technical Sciences, Associate Professor at Voronezh Institute of High Technologies, Voronezh, Russian Federation.

*Статья поступила в редакцию 03.10.2022; одобрена после рецензирования 31.10.2022; принята к публикации 23.11.2022.*

*The article was submitted 03.10.2022; approved after reviewing 31.10.2022; accepted for publication 23.11.2022.*