УДК 004.056:519.86

5.2.2. Математические, статистические и инструментальные методы экономики (физико-математические науки, экономические науки)

КОМПЛЕКС ЭКОНОМИКО-МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Титов Александр Юрьевич
руководитель отдела информационной безопасности
SPIN – код автора: 6939-9736
ООО «Радиус» г. Белгород, Россия

В статье представлен комплекс экономико-математических моделей, направленных на формализацию и количественную оценку уровня информационной безопасности на основе обработки данных журналов угроз. Разработаны: модель построения законов распределения вероятностей случайных величин, модель генерации выборок на их основе, модель стохастического автомата, функционирующего в случайной среде, а также модель вычисления нормы, характеризующей уровень информационной защищённости. Описанные модели функционируют в составе информационной системы и обеспечивают возможность имитационного анализа, оценки вероятностных характеристик угроз, а также формирования обоснованных решений в сфере ИБ при наличии неопределённости. Практическая ценность работы заключается в создании формализованного инструментария для повышения обоснованности решений в области управления информационной безопасностью

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СТОХАСТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, СЛУЧАЙНЫЕ ВЕЛИЧИНЫ, УГРОЗА, ЗАКОН РАСПРЕДЕЛЕНИЯ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

http://dx.doi.org/10.21515/1990-4665-211-049

UDC 004.056:519.86

5.2.2. Mathematical, statistical and instrumental methods of economics (physical and mathematical sciences, economic sciences)

SET OF ECONOMIC-MATHEMATICAL MODELS FOR ASESSING INFORMATION SECURITY LEVEL

Titov Alexander Yuryevich
Head of the Information Security Department
RSCI SPIN-code: 6939-9736
Radius LLC, Belgorod, Russia

This article presents a set of economic-mathematical models designed to formalize and quantitatively assess the level of information security through the processing of threat log data. The following models are developed: a model for constructing probability distribution laws of random variables, a model for generating samples based on these distributions, **a** stochastic automaton model operating in a random environment, and a model for computing a norm characterizing the level of information security protection**.** The described models operate within an information system, enabling simulation analysis, assessment of probabilistic threat characteristics, and the formation of well-founded decisions in the field of information security under conditions of uncertainty. The practical value of the work lies in creating a formalized toolkit to enhance the substantiation of decisions in information security management

Keywords: INFORMATION SECURITY, SIMULATION MODELING, STOCHASTIC AUTOMATON, RANDOM VARIABLES, THREAT, DISTRIBUTION LAW

Введение

В условиях стремительного развития цифровой экономики информационная безопасность приобретает статус ключевого фактора устойчивого функционирования организаций и национальных инфраструктур. Рост объёмов обрабатываемой информации, повышение зависимости бизнес-процессов от цифровых систем, а также усложнение и интенсификация ки-

беругроз создают необходимость в разработке научно обоснованных методов оценки и управления уровнем защищённости. Традиционные подходы зачастую не позволяют адекватно учитывать вероятностную природу угроз и неопределённость внешней среды, что ограничивает эффективность принимаемых решений. В связи с этим возрастает значимость экономико-математического моделирования как инструмента для анализа, прогнозирования и оптимизации процессов обеспечения информационной безопасности. Комплекс моделей, рассматриваемый в настоящем исследовании, направлен на повышение точности и обоснованности оценки рисков и угроз с учётом их вероятностных характеристик.

Значение информационной безопасности в современном мире

С ускорением цифровизации всех сфер жизнедеятельности возникает новая угроза — цифровая уязвимость. Если несколько десятилетий назад основными мишенями для атак становились физическая инфраструктура и материальные ресурсы, то сегодня ключевыми объектами становятся цифровые системы, каналы передачи данных и персональные устройства. Всё больше секторов экономики зависит от работы с данными, а следовательно, угроза потерять эти данные или нарушить их целостность становится критической. Например, кибератаки на финансовые учреждения могут парализовать работу банковских систем и вызвать обрушение финансовых рынков. Аналогично, взломы в области здравоохранения могут привести к потере медицинских данных и негативно сказаться на здоровье населения. Такие инциденты подтверждают, что для поддержания экономической стабильности необходимо учитывать риски, связанные с информационными атаками.

Современное движение общества в сторону цифровизации позволяет значительно ускорить все процессы экономического развития. В рамках реализации Указов Президента Российской Федерации от 7 мая 2018 г № 204 «О национальных целях и стратегических задачах развития Россий-

ской Федерации на период до 2024 года» и от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации на базе программы «Цифровая экономика Российской Федерации» сформирована национальная программа «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

Национальная программа включает в себя семь федеральных проектов: «Нормативное регулирование цифровой среды», «Информационная инфраструктура», «Кадры для цифровой экономики», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление» и «Искусственный интеллект».

В структуру национального проекта «Цифровая экономика» входят следующие федеральные проекты [1]:

1. Нормативное регулирование цифровая среды.
2. Информационная инфраструктура.
3. Кадры для цифровой экономики.
4. Информационная безопасность.
5. Цифровые технологии.
6. Цифровое государственное управление.

В представленный перечень проектов включен пункт, посвященный информационной безопасности, что еще раз подчеркивает важность данного вопроса в современных условиях.

Цели и задачи статьи

Цель настоящей статьи: представить разработанный интегрированный комплекс экономико-математических моделей для оценки уровня информационной безопасности, наглядно продемонстрировать его архитектуру (с использованием блок-схем) и верифицировать работоспособность. Комплекс моделей использует имитационную модель, построенную на данных журнала угроз, для генерации адекватных распределений ключевых случайных величин (частота инцидентов), повышая достоверность оценки рисков, оптимизации затрат и расчета интегрального уровня ИБ в целях поддержки экономически обоснованных управленческих решений.

Указанную цель планируется достигнуть посредством решения следующих задач:

1. Представить концептуальную архитектуру разработанного интегрированного комплекса экономико-математических моделей оценки уровня ИБ.
2. Описать функциональное назначение, логику работы и ключевые алгоритмы каждого компонента комплекса, особое внимание уделив имитационной модели.
3. Наглядно представить структуру имитационной модели и взаимодействие его компонентов.
4. Описать методику практического применения имитационной модели (последовательность шагов, использование результатов каждого компонента).
5. Провести верификацию и демонстрацию работоспособности имитационной модели.

Концептуальная модель информационной системы анализа уровня информационной безопасности хозяйствующих субъектов представлена на рисунке 1. В состав информационной системы включён комплекс эконо-

мико-математических моделей $M =< M_1, M_2, M_3, M_4 >$, позволяющих прогнозировать вероятность уязвимостей информационной системы.

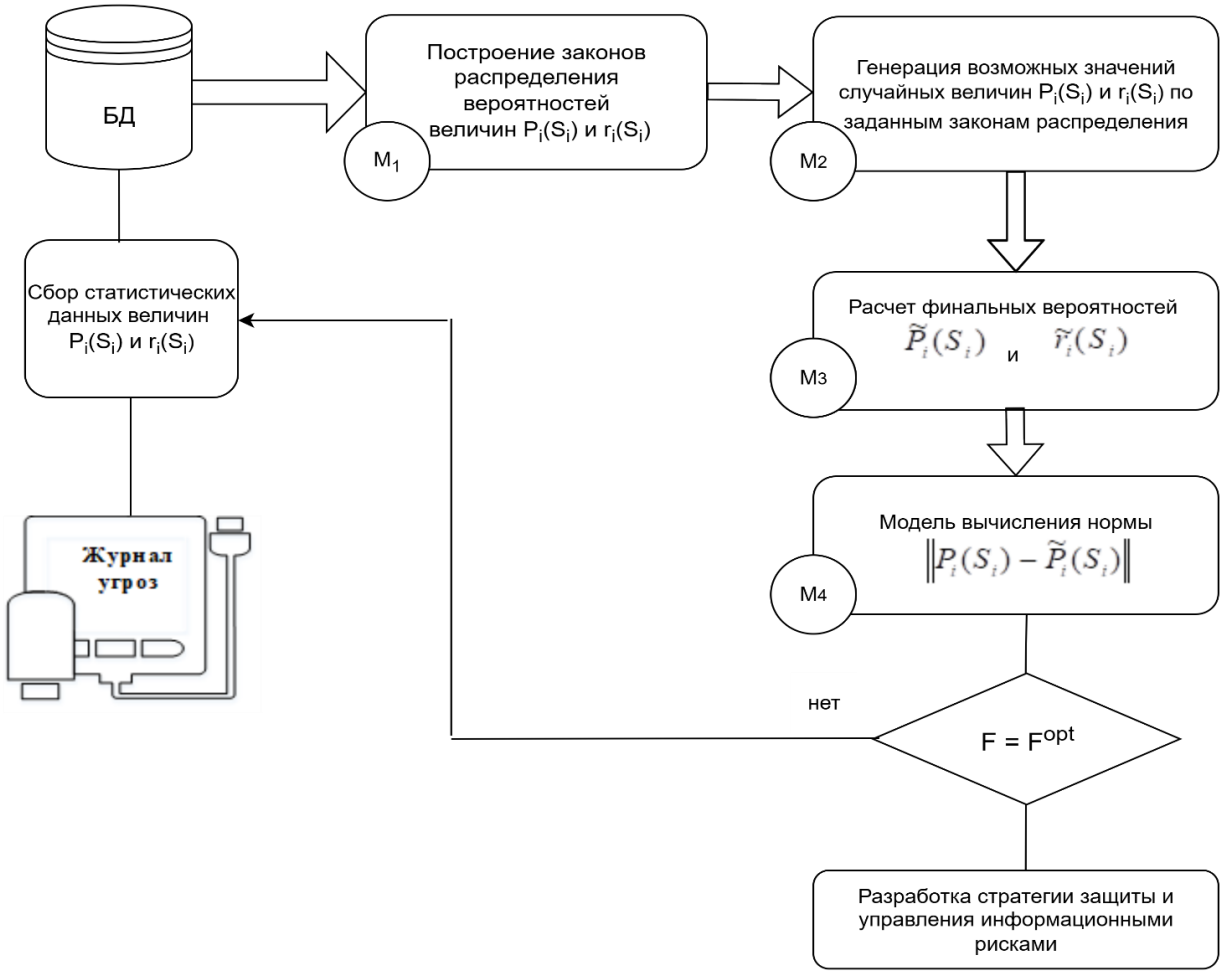

Рисунок 1 – Концептуальная модель информационной системы анализа уровня информационной безопасности хозяйствующих субъектов

В состав комплекса $M =< M_1, M_2, M_3, M_4 >$ включены следующие экономико-математические модели:

1. M_1- модель построения законов распределения вероятностей случайных величин $P_i(S_i)$ и $r_i(S_i)$, значения которых получены из журнала угроз.

2. M_2 - модель генерации возможных значений случайных величин $P_i(S_i)$ и $r_i(S_i)$ по заданным законам распределения.

3. M_3 - модель стохастического автомата, функционирующего в случайной среде, результатом работы которого является получение финальных вероятностей величин $\widetilde{P}_i(S_i)$ и $\widetilde{r}_i(S_i)$

4. M_4 - модель вычисления нормы $\left\|P_i(S_i) - \widetilde{P}_i(S_i)\right\|$.

Настоящая работа является частью более широкого исследования, направленного на разработку комплекса экономико-математических моделей оценки уровня информационной безопасности. В рамках данной статьи подробно рассматривается одна из моделей — «Имитационная модель построения законов распределения вероятностей возникновения угроз».

Ранее в своих статьях автор поднимал проблему оценки уровня информационной безопасности посредством применения математических моделей и методов. В соответствии с приведённым в статье «Математическая модель оценки информационной безопасности хозяйствующих субъектов» [2] графом состояний системы оценки уровня информационной безопасности, информационная система хозяйствующего субъекта переходит из устойчивого состояния S_0 в состояния наличия угроз S_i, $i=\overline{1,n}$, когда различные угрозы приходят с вероятностями P_{oi}. В этой статье изложены результаты построения законов распределения вероятностей угроз P_{oi}, составляющих основу модели $M_1 \in M$. Исходными данными модели M_1 являются выборки V^i, $i=\overline{1,n}$, полученные из журналов угроз: $V^i = \{v_1^i, v_2^i, ..., v_k^i\}$, где v_j^i, $j=\overline{1,k}$ – периодические (ежедневные) значения количества угроз, воздействующих на хозяйствующий субъект. На основе

значений $V^i = \{v_1^i, v_2^i, ..., v_k^i\}$ определяются вероятности $H^i = \{h_1^i, h_2^i, ..., h_k^i\}$ угрозы вида i: $h_j^i = \frac{\sum_{j=1}^{k} h_j^i}{k}$.

Имитационное моделирование, типы имитационных моделей

Имитационное моделирование представляет собой мощный инструмент, позволяющий исследовать сложные системы и процессы, которые трудно анализировать традиционными математическими методами. В контексте информационной безопасности имитационные модели позволяют воссоздать динамику взаимодействия между различными элементами системы, включая пользователей, программное обеспечение и потенциальные угрозы.

Основная цель имитационного моделирования в области информационной безопасности заключается в оценке уровня рисков и уязвимостей, а также в разработке стратегий для их минимизации. Имитационные модели дают возможность исследовать различные сценарии атак, оценивать последствия инцидентов и тестировать эффективность мер по защите информации.

Рассмотрим основные типы имитационных моделей, применяемых в данной области.

1. Дискретно-событийные модели (Discrete Event Simulation, DES). Дискретно-событийные модели описывают систему через последовательность отдельных событий, каждое из которых вызывает изменение состояния системы. В контексте информационной безопасности такие модели позволяют воспроизвести последовательность атак, реакции системы защиты и временные интервалы между событиями.

Пример применения: моделирование атаки на сеть с последующим реагированием системы защиты, определение времени восстановления после инцидента.

Преимущества: высокая точность при моделировании процессов с четко определенными событиями и временными интервалами.

Модели такого вида довольно часто применяются в различных исследовательских областях. Так в статье «Дисктерно-событийное моделирование для систем метро» [3] авторами описывается модель пассажиропотоков в метро, основанная на дискретных событиях. Вместо того чтобы искусственно создавать входные данные, авторы используют готовые исторические данные – так называемые матрицы корреспонденции.

2. Модели системной динамики (System Dynamics). Эти модели используют дифференциальные уравнения для описания взаимодействий между компонентами системы во времени. Они позволяют анализировать долгосрочные тренды и влияние стратегических решений на уровень информационной безопасности.

Пример применения: оценка влияния инвестиций в защиту на снижение риска утечки данных за длительный период.

Преимущества: подходит для стратегического планирования и оценки эффектов политики безопасности.

В статье «Построение моделей системной динамики в условиях ограниченной экспертной информации» [4] представлен метод разработки моделей системной динамики. Этот метод, основанный на подходе Л. В. Канторовича к математической обработке данных, представляет собой комплекс математических моделей и вычислительных алгоритмов. Он позволяет исследователю включать ключевые факторы, влияющие на точность модели. Апробация метода проведена на примере моделирования населения Российской Федерации.

3. Агентные модели (Agent-Based Modeling). Агентные модели основаны на моделировании поведения множества агентов — пользователей, злоумышленников или системных компонентов — с их собственными правилами взаимодействия.

Пример применения: моделирование поведения злоумышленников при попытках проникновения и реакции системы защиты.

Преимущества: позволяет учитывать сложное поведение участников системы и их взаимодействия, что важно при анализе современных киберугроз.

В то время как системная динамика и дискретно-событийное моделирование анализируют систему в целом ("сверху вниз"), агентное моделирование, получившее распространение после 2000 года, действует "снизу вверх", моделируя поведение отдельных объектов (агентов) [5].

Проведенный анализ типов имитационного моделирования позволил выявить характерные особенности, представленные в таблице 1.

Результаты анализа типов имитационного моделирования показывают, что их применение позволяет формализовать и получить количественно обоснованное, комплексное представление о состоянии информационной безопасности организации на разных уровнях. Адресное использование моделей– системной динамики для стратегических сценариев, дискретно-событийного подхода для аудита процессов ИБ, агентного моделирования для анализа угроз, связанных с поведением, –в совокупности создает основу для всесторонней оценки уровня защищенности. Это обеспечивает переход от интуитивных к строго формализованным и доказательным решениям в управлении информационной безопасностью, что позволяет получить комплексное представление о состоянии информационной безопасности организации. Выбор конкретной модели зависит от целей исследования: стратегического планирования, оценки рисков или анализа поведения участников системы. В совокупности они обеспечивают более точную и обоснованную оценку уровня защищенности информационных систем.

Таблица 1 - Ключевые различия в типах имитационного моделирования

Характеристика	**Системная динамика (SD)**	**Дискретно-событийное (DES)**	**Агентное (ABM)**
Уровень анализа	Макро (система в целом)	Мезо (процессы, ресурсы)	Микро (индивидуумы)
Основные элементы	Запасы, Потоки, Обратные связи	События, Очереди, Ресурсы, Транзакты (сущности)	Агенты, Правила, Среда, Взаимодействия
Подход	"Сверху-вниз"	Фокус на процессах	"Снизу-вверх"
Детализация	Низкая (агрегированная)	Средняя (логика процессов)	Высокая (агенты)
Время	Непрерывное/Дискретное (крупный шаг)	Дискретное (события)	Обычно дискретное (шаг)
Ключевой феномен	Обратные связи, Тренды	Очереди, Загрузка ресурсов, Временные задержки	Возникающее поведение, Самоорганизация, Сложность
Типичные задачи	Стратегическое планирование, Долгосрочные эффекты	Оптимизация процессов, Анализ производительности, Управление ресурсами	Изучение сложных систем, Социальные феномены, Адаптивное поведение

Имитационная модель построения законов распределения вероятностей возникновения угроз

Ключевым этапом в оценке уровня ИБ является формализация частоты и характера возникновения угроз. Поскольку априорные данные о законах распределения часто отсутствуют или ненадежны, основу модели составляет процедура построения эмпирических законов распределения вероятностей непосредственно из обрабатываемых данных журналов угроз.

Сама процедура построения эмпирического закона распределения вероятностей угроз представляет собой последовательность следующих шагов.

Шаг1. Определяется размах варьирования величин $H^i = \{h_1^i, h_2^i, \dots, h_k^i\}$в виде $\Delta(h^i) = (h_j^{\max} - h_j^{\min})$.

Шаг2. Величина $\Delta(h^i)$ разбивается на m равных отрезков длиной $\lambda(h^i) = \frac{h^i_{\max} - h^i_{\min}}{m}$

Шаг 3. Определяются координаты декомпозированных отрезков: $\hat{h}^i_0 = 0;$ $\hat{h}^i_j = h^i_{\min} + \lambda(h^i) \cdot j;$

Шаг 4. Вычисляются координаты центров декомпозированных отрезков: $\bar{h}^i_j = h^i_0 + \frac{2j-1}{2}\lambda(h^j)$.

Шаг5. Вычисляется относительная частота попадания выборочных данных $H^i = \{h^i_1, h^i_2, ..., h^i_k\}$ в каждый из декомпозированных отрезков $\hat{h}^i_j$: $\alpha_j = \frac{\mu_j(\hat{h}^i_j)}{k}$, где k – длина выборки $H^i = \{h^i_1, h^i_2, ..., h^i_k\}$, μ_j – количество выборочных данных, попавших в декомпозированный отрезок $\hat{h}^i_j$.

Построенный эмпирический закон распределения вероятностей представлен в виде ряда распределения (Таблица 2)

Таблица 2 − Эмпирический закон распределения вероятностей случайной величины $H^i = \{h^i_1, h^i_2, ..., h^i_k\}$

$\bar{h}^i_j$	$\bar{h}^i_1$	$\bar{h}^i_2$	$\bar{h}^i_3$	…	$\bar{h}^i_z$
α_j	α_1	α_2	α_3	…	α_z

На рисунке 2 представлен алгоритм построения законов распределения вероятностей угроз в виде блок-схемы.

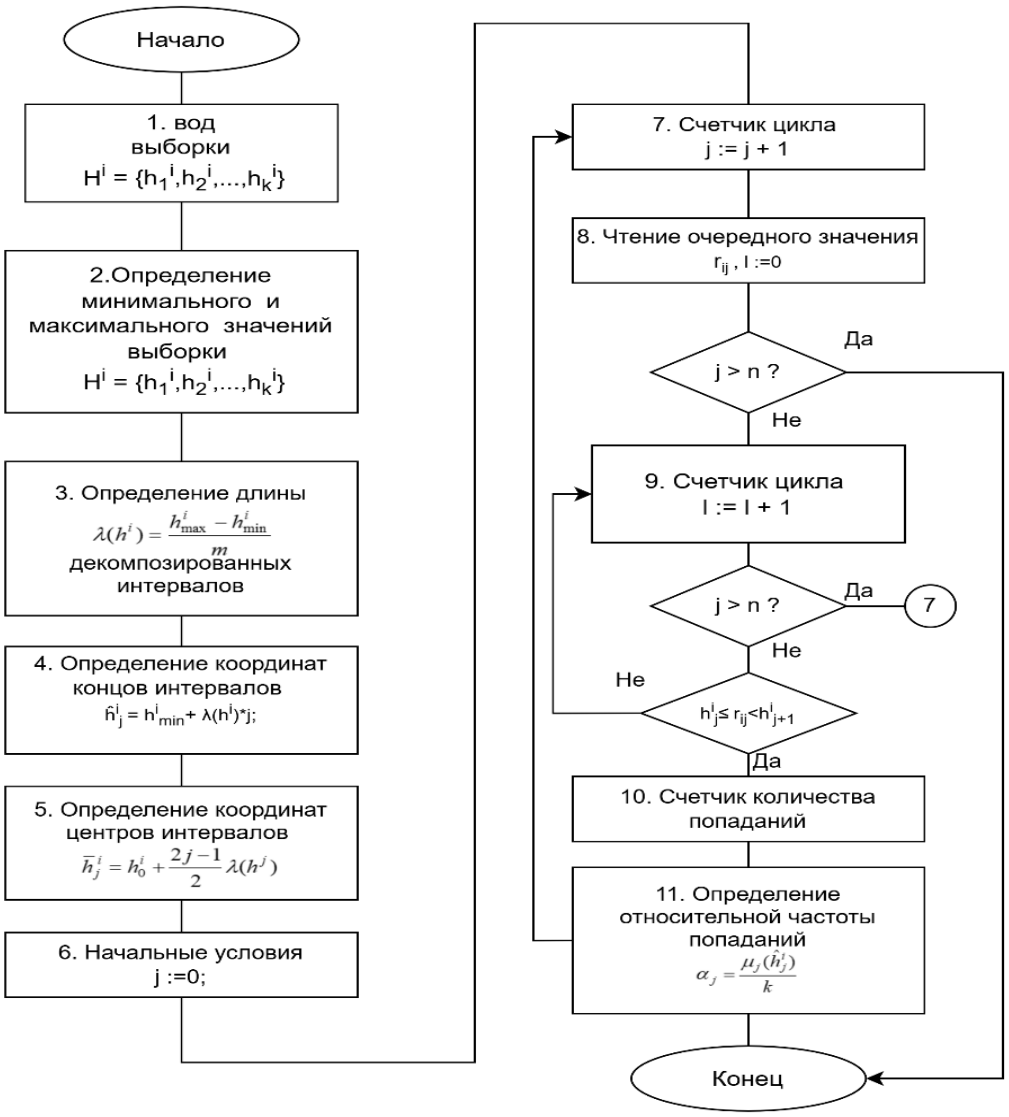

Рисунок 2 − Алгоритм построения законов распределения вероятностей угроз

Построенные эмпирические законы распределения используются в качестве исходных данных для генерации возможных значений вероятностей угроз.

Результаты и выводы

В данном разделе проводится верификация корректности функционирования и демонстрация практической работоспособности имитационной модели. Процесс запуска модели является интуитивным, при этом пользователь задает требуемый период исследования (количество прогонов) и инициирует расчет нажатием кнопки «ИМИТИРОВАТЬ». Ключе-

вым результатом является успешное получение и интерпретация выходных данных модели (распределения вероятностей возникновения угроз, траектории стохастического автомата, расчетные значения нормы защищенности). Сравнительный анализ этих результатов с историческими данными угроз и логикой моделируемых процессов показал их адекватность, подтверждая пригодность модели для решения задач оценки уровня ИБ.

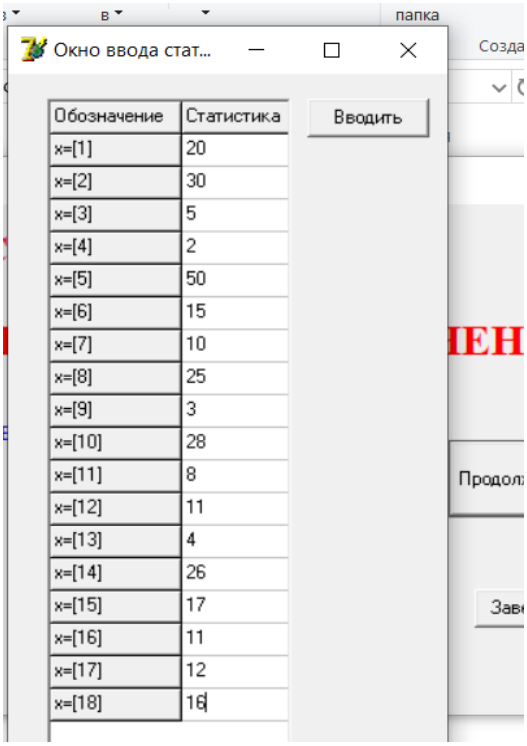

Рисунок 3 – Окно ввода информации о количестве угроз

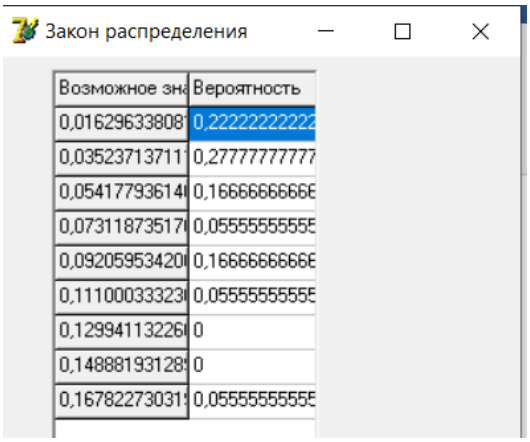

Рисунок 4 – Закон распределения вероятностей угроз «Вредоносное программное обеспечение»

Сгенерированные значения вероятностей угроз P_{oi} используются в качестве исходных данных для вычисления финальных вероятностей нахождения информационной системы хозяйствующего субъекта в безопасном состоянии S_0, в состоянии воздействия угрозы S_i вида i, а также в опасном состоянии S_{n+i} под воздействием угрозы вида i.

Заключение

Проведенное исследование подтверждает, что имитационное моделирование служит мощным и необходимым инструментом для комплексной оценки уровня информационной безопасности. Разработанный в работе формализованный комплекс экономико-математических моделей, ключевым элементом которого является стохастическая имитационная модель (включая построение эмпирических распределений угроз и функционирование автомата в случайной среде), позволяет:

1. Перейти от интуитивных к количественно обоснованным оценкам защищенности информационных систем.
2. Выявлять скрытые уязвимости и паттерны возникновения угроз на основе анализа реальных данных журналов.
3. Проводить сценарный анализ эффективности различных стратегий защиты до их реализации в реальной среде.

Таким образом, способность к прогнозированию и оценке последствий управленческих решений в условиях неопределенности становится критически важной в контексте постоянно эволюционирующего ландшафта угроз ИБ. Практическая ценность подхода заключается в создании формализованного, основанного на данных инструментария, который существенно повышает обоснованность решений в области управления информационной безопасностью, способствуя оптимальному распределению ресурсов и минимизации рисков.

Список цитируемой литературы

1. Национальный проект Цифровая экономика http://static.government.ru/media/files/3b1AsVA1v3VziZip5VzAY8RTcLEbdCct.pdf

2. Стрельцова Е.Д., Титов А.Ю., Яковенко И.В. Математическая модель оценки информационной безопасности хозяйствующих субъектов // Друкеровский вестник. - 2024. - № 2. - С. 182-193 http://dx.doi.org/10.17213/2312-6469-2024-2-182-193

3. Покусаев О. Н., Намиот Д. Е., Чекмарев А. Е. Дисктерно-событийное моделирование для систем метро // International Journal of Open Information Technologies. 2021. №7. URL: https://cyberleninka.ru/article/n/diskretno-sobytiynoe-modelirovanie-dlya-sistemy-metro (дата обращения: 23.07.2025).

4. О. Г. Кантор, С. И. Спивак, Построение моделей системной динамики в условиях ограниченной экспертной информации, Информ. и её примен., 2014, том 8, выпуск 2, С. 111–121

5. Лебедюк Э.А. АГЕНТНОЕ МОДЕЛИРОВАНИЕ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ. Вестник Российского экономического университета имени Г. В. Плеханова. 2017;(6):155-162. https://doi.org/10.21686/2413-2829-2017-6-155-162

References

1. Nacional'nyj proekt Cifrovaja jekonomika http://static.government.ru/media/files/3b1AsVA1v3VziZip5VzAY8RTcLEbdCct.pdf

2. Strel'cova E.D., Titov A.Ju., Jakovenko I.V. Matematicheskaja model' ocenki informacionnoj bezopasnosti hozjajstvujushhih sub#ektov // Drukerovskij vestnik. - 2024. - № 2. - S. 182-193 http://dx.doi.org/10.17213/2312-6469-2024-2-182-193

3. Pokusaev O. N., Namiot D. E., Chekmarev A. E. Diskterno-sobytijnoe modelirovanie dlja sistem metro // International Journal of Open Information Technologies. 2021. №7. URL: https://cyberleninka.ru/article/n/diskretno-sobytiynoe-modelirovanie-dlya-sistemy-metro (data obrashhenija: 23.07.2025).

4. O. G. Kantor, S. I. Spivak, Postroenie modelej sistemnoj dinamiki v uslovijah ogranichennoj jekspertnoj informacii, Inform. i ejo primen., 2014, tom 8, vypusk 2, C. 111–121

5. Lebedjuk Je.A. AGENTNOE MODELIROVANIE: SOSTOJaNIE I PERSPEKTIVY. Vestnik Rossijskogo jekonomicheskogo universiteta imeni G. V. Plehanova. 2017;(6):155-162. https://doi.org/10.21686/2413-2829-2017-6-155-162