УДК 004.056:519.854.2;519.237.5:004.056

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

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ПРОГНОЗИРОВАНИЯ КИБЕРАТАК ИНФОРМАЦИОННЫХ СИСТЕМ

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

Статья посвящена актуальной теме построения математических моделей, позволяющих предсказывать количество кибератак (фишинга и DDoS), направленных на дезорганизацию функционирования информационных систем. Формулировка задачи состоит в использовании исторических данных для создания прогноза. В процессе моделирования использовались методы классической линейной регрессии (LR) и авторегрессионной интегрированной скользящей средней (ARIMA). Приведено математическое описание применяемых методов, реализованных в виде программного продукта PROGNOS. На основе использования построенного программного продукта проведена серия машинных экспериментов с использованием исторических данных о количестве фишинговых и DDoS-атак. Проведена оценка качества прогнозирования на базе применяемых для составления прогноза методов LR и ARIMA. Результаты моделирования визуализированы на графиках. Практическая значимость результатов исследования состоит в возможности использования построенных моделей в системах предупреждения киберугроз

Ключевые слова: КИБЕРАТАКИ, ПРОГНОЗ, МАТЕМАТИЧЕСКИЕ МОДЕЛИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

http://dx.doi.org/10.21515/1990-4665-210-034

UDC 004.056:519.854.2;519.237.5:004.056

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

MATHEMATICAL MODELS FOR FORECASTING CYBER-ATTACKS OF INFORMATION SYSTEMS

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

The article is devoted to the current topic of constructing mathematical models that allow predicting the number of cyberattacks (phishing and DDoS) aimed at disrupting the functioning of information systems. The formulation of the problem consists in using historical data to create a forecast. In the process of modeling, the methods of classical linear regression (LR) and autoregressive integrated moving average (ARIMA) were used. A mathematical description of the methods used, implemented in the form of the PROGNOS software product, is given. Based on the use of the constructed software product, a series of machine experiments were conducted using historical data on the number of phishing and DDoS attacks. The forecast quality was assessed based on the LR and ARIMA methods used to make the forecast. The modeling results were visualized on graphs. The practical significance of the research results lies in the possibility of using the constructed models in cyber threat prevention systems

Keywords: CYBER ATTACKS, FORECAST, MATHEMATICAL MODELS, INFORMATION SECURITY

Введение

В современных реалиях, когда информационные технологии используются во всех сферах деятельности, обеспечение безопасности функционирования информационных систем и технология становится

одним из главных факторов обеспечения устойчивости работы компаний. Кибератаки любого типа, особенно фишинговые атаки и атаки типа «отказ в обслуживании (DDoS)», наносят значительный ущерб организациям. Это ставит проблему прогнозирования кибератак в категорию исключительно важных задач, позволяющих своевременно и оперативно обнаруживать потенциальные риски и разрабатывать модели и системы по их предотвращению. В последнее время фишинговые атаки становятся всё более изощрёнными. Нацеливаясь на похищение конфиденциальной информации, они используют социальную инженерию и другие уловки при манипуляции пользователями. Подобные действия делают фишинговые атаки особенно угрожающими. Не менее опасными являются DDoS-атаки, направленные на перегрузку систем и ресурсов. Действия DDoS атак приводят к значительным сбоям в работе IT систем и, как следствие, к потере доверия со стороны клиентов. В условиях дальнейшего роста кибератак и их разнообразия особую важность приобретает разработка и использование математических моделей, базирующихся на методах прогнозирования. Использование этих методов, являющихся критически важным для управления безопасностью IT систем, позволяет организациям принимать превентивные меры для защиты своих ресурсов. Следовательно, построение математических моделей прогнозирования кибератак, особенно фишинговых и DDoS-атак, актуализирует задачу в рамках комплексного подхода с применением современных технологий. Актуальность задачи прогнозирования количества кибератак способствовала появлению множества научных публикаций, посвящённых этой теме. Описание общего подхода и модели прогнозирования с использованием нейронечёткой сети приведено в [1]. Автором определены различные классы целей атак и сформирован набор признаков, характеризующих модели прогнозирования. Исследованию возможностей и ограничений использования методов теории временных

рядов для анализа и прогнозирования динамики кибератак посвящена статья [2]. Автором высказана и проверена гипотеза о влиянии характера исходных данных на выбор методов прогнозирования количества кибератак. На основе проведённых исследований построены модели прогнозирования количества кибератак, встроенные в информационную систему управления вузом. Разработке алгоритмов машинного обучения и их применения в области информационной безопасности посвящены работы [3,4,5]. В статье исследуются различные типы кибератак, которые могут быть предсказаны с помощью математического аппарата машинного обучения. Общие вопросы использования Искусственного интеллекта в вопросах кибербезопасности рассматривается авторами статьи [6]. Автором приведены таксономия и примеры организации кибербезопасности. Применению математического аппарата нечёткой логики и созданию на их основе моделей обеспечения информационной безопасности посвящены исследования [7,8,9,10,11].

Авторами разработаны общие подходы к постановке задач моделирования объектов защиты информационных систем, функционирующих в хозяйственных субъектах. Приведены алгоритмы информационных технологий, обеспечивающих защиту цифровой информации. Несмотря на обилие научных публикаций по данной тематике, в них не охватываются все возникающие проблемы, что подчёркивает необходимость проведения дополнительных исследований. В данной статье предложен подход к построению математических моделей прогнозирования количества кибератак на основе обработки временных рядов, полученных в результате наблюдения за работой информационных систем обеспечения информационной безопасности. Статья структурирована следующим образом. Во введении обоснована актуальность исследований по построению математических моделей прогнозирования кибератак. В разделе «Модели и методы» приведено математическое описание метода

классической линейной регрессии и метода ARIMA (Autoregressive Integrated Moving Average), применяемых для предсказания количества фишинговых и DDoS атак. В статье продемонстрированы результаты экспериментов, проведённых на построенных математических моделях прогнозирования кибератак.

Модели и методы

В данной работе используются два подхода к прогнозированию кибератак:

- классической линейной регрессии (LR);
- модели ARIMA (Autoregressive Integrated Moving Average).

Исследование базируется на анализе временных рядов, включающих ежемесячные данные о количестве фишинговых и DDoS-атак за период 2020-2023 годы. Особое внимание уделяется выявлению и учёту трендовых компонент, а также анализу автокорреляционной структуры данных. Рассмотрим применяемые в работе методы.

Метод классической линейной регрессии

Метод классической линейной регрессии (LR) исходит из предположения линейной зависимости целевой переменной y (количество атак) от признаков x (временной ряд с номерами месяцев) $y_i = \beta_0 + \beta_1 \cdot x_i + \varepsilon_i$,

где y_i – количество атак в момент i;

x_i – временная метка (номер месяца);

β_0, β_1 – коэффиенты (интерсепт и наклон);

ε_i –ошибка.

Для нахождения коэффициентов β_0, β_1 применяется метод наименьших квадратов, который работает, исходя из минимизации суммы квадратов ошибок $S = \min\limits_{\beta_0,\beta_1} \sum\limits_{i=1}^{n} (y_i - (\beta_0 + \beta_1 x_i))^2$. Нахождение минимума S

осуществляется с помощью частных производных $\frac{\partial S}{\partial \beta_0}$, $\frac{\partial S}{\partial \beta_1}$. Выполняя дифференцирование, подучим следующее.

$$\frac{\partial S}{\partial \beta_0} = -2\sum_{i=1}^{n}(y_i - \beta_0 - \beta_1 x_i) = 0;$$

$$\sum_{i=1}^{n} y_i - n\beta_0 - \beta_1 \sum_{i=1}^{n} x_i = 0;$$

$$n\beta_0 + \beta_1 \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i;$$

$$\frac{\partial S}{\partial \beta_1} = -2\sum_{i=1}^{n} x_i(y_i - \beta_0 - \beta_1 x_i) = 0.$$

$$\sum_{i=1}^{n} x_i y_i - \beta_0 \sum_{i=1}^{n} x_i - \beta_1 \sum_{i=1}^{n} x_i^2 = 0;$$

$$\beta_0 \sum_{i=1}^{n} x_i + \beta_1 \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} x_i y_i.$$

В итоге составляется система уравнений:

$$\begin{cases} n\beta_0 + \beta_1 \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i \\ \beta_0 \sum_{i=1}^{n} x_i + \beta_1 \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} x_i y_i \end{cases}$$

Решение этой системы приводит к следующим аналитическим выражениям для β_0, β_1:

$$\beta_0 = \frac{\sum_{i=1}^{n} y_i - \beta_1 \sum_{i=1}^{n} x_i}{n}; \quad \beta_1 = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2};$$

$$\beta_0 = \bar{y} - \beta_1 \bar{x}; \quad \bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}; \quad \bar{y} = \frac{\sum_{i=1}^{n} y_i}{n}.$$

После вычисления коэффициентов β_0 и β_1 модель $y_i = \beta_0 + \beta_1 x_i$ готова к прогнозированию. Для оценки качества необходимо подставить известные значения x_i и рассчитать среднеквадратичную ошибку $MSE = \frac{\sum_{i=1}^{n}(y - y_i)^2}{n}$,

где y – прогноз; y_i – реальное значение; n –количество наблюдений.

Для прогнозирования количества атак y необходимо задать y_i для месяцев, которых нет в данных. Преимущества метода классической линейной регрессии (LR) состоят в следующем:

- простота;
- в модели легко интерпретировать коэффициенты;
- вычислительная эффективность: модель быстро обучается даже на больших данных;
- устойчивость из-за малого количества гиперпараметров для настройки.

Но модель (LR) обладает рядом недостатков:

- модель предполагает линейность и не подходит для сложных нелинейных трендов;
- в модели не учитывается зависимость между последовательными точками;
- является чувствительной к выбросам, т.к. квадратичная ошибка усиливает влияния аномалий.

В связи с наличием этих недостатков в работе для прогнозирования кибератак, в дополнение модели (LR) предложена модель, созданная на основе метода ARIMA (AutoRegressive Integrated Moving Average).

Метод ARIMA

Метод ARIMA сочетает в себе три ключевых компонента: авторегрессию (AR), интегрированную часть (I) и скользящее среднее (MA). Опишем каждую из этих компонентов.

Авторегрессия (AR(p))

Эта составляющая, обозначаемая как AR(p) моделирует текущее значение временного ряда посредством линейной комбинации от его предыдущих значений:

$$x(t) = \phi_1 x_{t-1} + \phi_2 x_{t-2} + ... + \phi_p x_{t-p} + \varepsilon_t$$

Величина p задаёт порядок авторегрессии.

Интегрирование (I(d))

Цель интегрирования–устранение нестационарности временного ряда, что позволяет применять методы, основанные на стационарности данных. Если временной ряд нестационарен, то применяется разностное преобразование. При этом первая разница временного ряда имеет вид: $y_t = x_t - x_{t-1}$, где y_t – разностный ряд. Порядок d отражает количество разностей, необходимых для достижения стационарности.

Скользящее среднее (MA(q))

Целью этого компонента является моделирование текущего значения временного ряда, как линейной комбинации предыдущих ошибок. Величина q в обозначении MA(q) означает порядок скользящего среднего. Текущее значение x_t определяется, исходя из выражения:

$$x_t = \mu_t + \varepsilon_t + \Theta_1 \varepsilon_{t-1} + \Theta_2 \varepsilon_{t-2} + ... + \Theta_q \varepsilon_{t-q}$$

где x_t – текущее значение временного ряда в момент времени t;

μ – среднее значение временного ряда;

ε_t – текущая ошибка (или шум) в момент времени t;

$\Theta_1, \Theta_2, ..., \Theta_p$ – коэффициенты скользящего среднего, которые определяют влияние предыдущих ошибок не текущее значение.

Коэффициенты $\Theta_1, \Theta_2, ..., \Theta_p$ представляют собой веса, которые применяются к ошибкам, которые произошли в предыдущие моменты времени. Каждый коэффициент Θ_i, $i = \overline{1, p}$ показывает, на сколько сильно

ошибка в момент времени t влияет на текущее значение. Таким образом, общая модель ARIMA обозначается ARIMA (p, d, q), где

p–порядок авторегрессии;

d – порядок интегрирования;

q– порядок скользящего среднего.

Обобщая изложение, можно записать модель ARIMA в следующем виде:

$$\Delta^d \cdot x_t = \phi_1 \cdot \Delta^d \cdot x_{t-1} + \phi_2 \cdot \Delta^d \cdot x_{t-2} + ... + \phi_p \cdot \Delta^d \cdot x_{t-p} + \varepsilon_t + \Theta_1 \cdot \varepsilon_{t-1} +$$
$$+\Theta_2 \cdot \varepsilon_{t-2} + ... + \Theta_p \cdot \varepsilon_{t-p}$$

где Δ^d – оператор разности, применяемый d раз.

Опишем ARIMA (1,1,1), применяемой в настоящих исследованиях для прогнозирования кибератак. Такая модель включает в себя следующие компоненты.

Авторегрессия AR (1)

В данной модели используется один лаг $p=1$, т.е. текущее значение временного ряда зависит от его предыдущего значения: $x_t = \phi_1 \cdot x_{t-1} + \varepsilon_t$.

Интегрирование I (1)

Параметр $d=1$указывает на то, что временной ряд x_t преобразовывался на основе первой разности с целью сделать его стационарным: $y_t = x_t - x_{t-1}$, где y_t–разностный ряд.

Скользящее среднее MA (1)

На этом этапе используется один лаг ошибки $q=1$, т.е. текущее значение временного ряда связывается с предыдущей ошибкой прогноза:

$x_t = \Theta_0 + \Theta_1 \cdot \varepsilon_{t-1} + \varepsilon_t$, где ε_t– белый шум (ошибка).

Объединение всех компонентов ARIMA (1,1,1) позволяет записать:

$$x_t = \phi_1 \cdot x_{t-1} + \Theta_1 \cdot \varepsilon_{t-1} + \varepsilon_t + c.$$

Основные преимущества модели ARIMAсостоят в следующем.

- ARIMA способна моделировать как стационарные, так и нестационарные данные;

- параметры AR, I, MA модели позволяют анализировать влияние различных факторов на временной ряд за счёт простоты их интерпретации. Методы классической линейной регрессии ARIMA программно реализованы в программном продукте PROGNOS на языке Phyton, что позволило проведению серии экспериментов для прогнозирования кибер-атак.

Результаты исследований и их обсуждение

Для проведения экспериментов с использованием программного продукта PROGNOS были собраны ежемесячные данные о количестве кибератак (фишинг и DDoS) за период с января 2020 года по февраль 2024 года (Таблица 1).

Таблица 1– Ежемесячные данные о количестве кибератак (фишинг и DDoS) за период с января 2020 года по февраль 2024 года

Месяц	Фишинг	DDoS	Месяц	Фишинг	DDoS
1	2	3	4	5	6
2020-01-31	4200	2100	2022-01-31	14000	9800
2020-02-29	4500|	2300	2022-02-28	14500	10300
2020-03-31	5000	2800	2022-03-31	15200	11000
2020-04-30	5400	|3000	2022-04-30	15800	11500
2020-05-31	5800	|3200	2022-05-31	16500	12000
2020-06-30	6200	|3500	2022-06-30	17200	12800
2020-07-31	6600	3800	2022-07-31	17900	13500
2020-08-31	5900	3600	2022-08-31	17500	13200
2020-09-30	6800	4000	2022-09-30	18500	14000
2020-10-31	7200	4500	2022-10-31	19200	14800
2020-11-30	7600	4800	2022-11-30	20000	15600
2020-12-31	8000	5000	2022-12-31	20800	16500
2021-01-31	8500|	5200	2023-01-31	21600	17400
2021-02-28	9000	9000|	2023-02-28	22500	18300
2021-03-31	9500	5800	2023-03-31	23500	19200
2021-04-30	10000	6100	2023-04-30	24500	20100
2021-05-31	10500	6500	2023-05-31	25600	21000
2021-06-30	11000	7000	2023-06-30	26800	22000
2021-07-31	11500	7500	2023-07-31	28000	23000
2021-08-31	11200	7200	2023-08-31	27500	22800
2021-09-30	12000	7800	2023-09-30	29000	24000
2021-10-31	12500	8300	2023-10-31	30500	25200
2021-11-30	13000	8800	2023-11-30	32000	26500
2021-12-31	13500	9300	2024-02-29	36500	30200

В процессе реализации моделей в программном продукте PROGNOS использовались временные метки $t = 1, 2, ..., 48$ (номера месяцев) и целевая

функция x_t. На рисунке 1 приведены графики кибератак, демонстрирующие исторические данные и прогнозы.

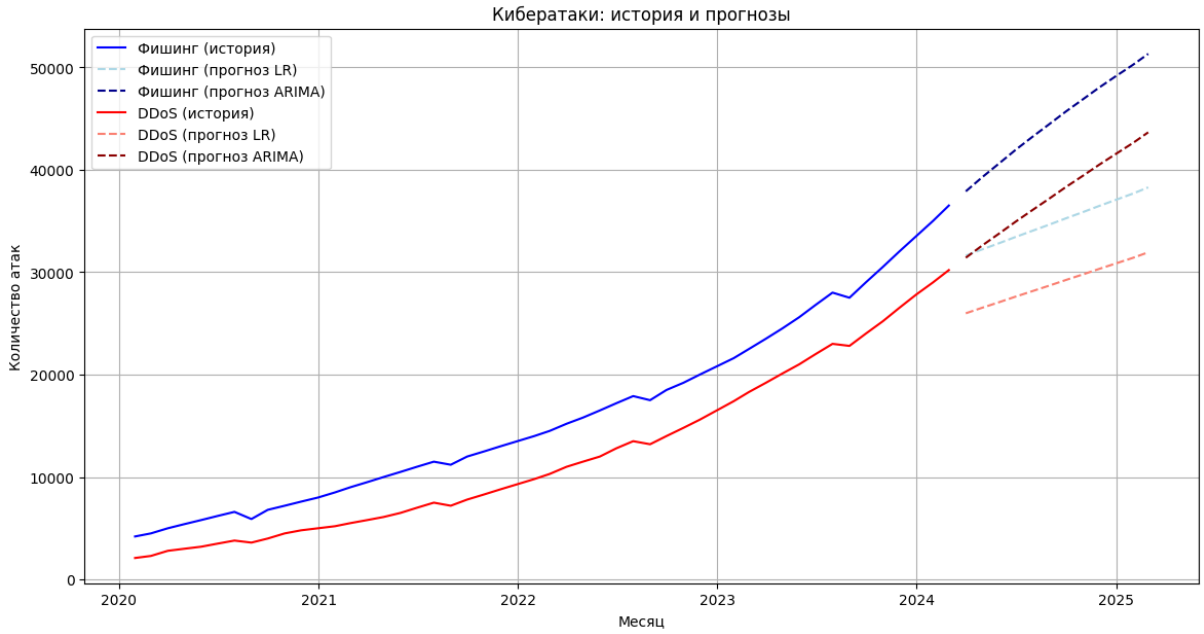

Рисунок 1 - Графики кибератак, демонстрирующие исторические данные и прогнозы

В таблице 2 приведены прогнозные значения кибератак, вычисленные по методам ARIMA и классической линейной регрессии (LR).

Таблица 2 – Прогнозные значения кибератак, вычисленные по методам ARIMA и классической линейной регрессии (LR)

Дата	Фишинг_LR	Фишинг_ARIMA	DDoS_LR	DDoS_ARIMA
2024-03-31	31613	37885	25981	31406
2024-04-30	32218	39261	26522	32597
2024-05-31	32824	40610	27063	33764
2024-06-30	33429	41926	27605	34915
2024-07-31	34034	43205	28146	36056
2024-08-31	34639	44449	28687	37183
2024-09-30	35245	45666	29228	38294
2024-10-31	35850	46852	29769	39391
2024-11-30	36455	48008	30310	40475
2024-12-31	37060	49134	30851	41546
2025-01-31	37665	50233	31393	42603
2025-02-28	38271	51304	31934	43646

Компьютерная программа PROGNOS оценивает точность прогнозирования, используя модели линейной регрессии (L)R и авторегрессионной интегрированной модели скользящего среднего (ARIMA), основываясь на метриках среднеквадратической ошибки (MSE, Mean Squared Error) и корня из среднеквадратической ошибки (RMSE, Root Mean Squared Error). Метрики MSE и RMSE рассчитываются с использованием следующих аналитических выражений:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - y_i)^2,\ RMSE = \sqrt{MSE};$$

где y_i – реальное значение количества кибератак;

y_i – предсказанное значение количества кибератак;

n – количество наблюдений.

Расчёт точности прогнозирования осуществляется, как

$$MAPE = \frac{100\%}{n}\sum_{i=1}^{n}\left|\frac{y_i - y_i}{y_i}\right|.$$

В результате функционирования программного обеспечения PROGNOS производится оценка точности прогнозирования на основе методов LR и ARIMA, учитывая данные о количестве фишинговых (Таблица 3) и DDoS-атак (Таблица 4).

Таблица 3– Оценка точности прогнозирования количества фишинговых атак на основе методов LR и ARIMA

	LR-Linear Regression	ARIMA
MSE	3634315.76	541111.74
RMSE	1906.39	735.60
MAPE (Точность (%))	87.19 %	95.64 %

Таблица 4– Оценка точности прогнозирования количества DDoS-атак на основе методов LR и ARIMA

	LR-Linear Regression	ARIMA
MSE	3726464.00	191056.11
RMSE	1930.41	437.10
MAPE (Точность (%))	76.39 %	95.32 %

Результаты оценки точности прогнозирования позволили сделать ввод, что, модель ARIMA (1,1,1) наиболее точно предсказывает количество фишинговых и DDoS атак. Удобство применения модели ARIMA (1,1,1) состоит в том, что она требует только одной разности для достижения стационарности.

Заключение

В ходе проведённых исследований разработаны и протестированы математические модели прогнозирования кибератак (фишинга и DDoS) с использованием методов классической линейной регрессии (LR) и авторегрессионной интегрированной скользящей средней (ARIMA). Приведено математическое описание используемых методов, на основе которых разработан программный продукт PROGNOS. С помощью программы PROGNOS проведены эксперименты с использованием исторических данных за 50 месяцев и построены прогнозы на 2024год. Проведена оценка точности моделей с помощью метрик MSE, RMSE и MAP. В ходе оценки точности моделей получены следующие ключевые выводы.

1. Применение метода ARIMA показала лучшие результаты по всем метрикам: точность 99.8 % для фишинга и 99.9 для DDoS-атак. Кроме того, ARIMA продемонстрировала устойчивость к нелинейным трендам (в отличие от линейной регрессии).

2. Линейная регрессия оказалась менее точной (98.5 для фишинга и 98.7 для DDoS-атак). Однако, эта модель является полезной для базовой оценки трендов.

Визуализация результатов моделирования подтвердила сделанные выводы. Следовательно, для критически важных систем рекомендуется использовать модель, построенную на методе ARIMA. Построенные модели, реализованные посредством программного кода PROGNOS, предоставляет инструментарий для антикризисного планирования кибербезопасности, позволяя предсказывать кибератаки.

В перспективе планируется продолжать исследования в направлении создания систем управления безопасностью информации и событиями (SIEM-систем), которые позволяют собирать, анализировать и хранить данные о безопасности из различных источников в реальном режиме времени.

Литература

1. Дойникова Е. В. Модель прогнозирования целей кибератак на основе нейронечётких сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 405-408.
2. Наумов В. Н. и др. Анализ и прогнозирование временных рядов кибератак на информационную систему ведомственного вуза: возможности и ограничения методов //Труды учебных заведений связи. – 2025. – Т. 11. – №. 1. – С. 99-112.
3. Мишин А. Е., Былевский П. Г. Применение машинного обучения для прогнозирования кибератак //Hi-Hume Journal. – 2023. – Т. 3. – С. 80.
4. Лощилин А. В., Яриков В. Г., Никишова А. В. методы машинного обучения в прогнозировании и предотвращении кибератак //NBI-technologies. – 2024. – Т. 18. – №. 2. – С. 33-39.
5. АСЯЕВ Г. Д., СОКОЛОВ А. Н. Модели предиктивной защиты информации автоматизированной системы управления водоснабжением на основе временных рядов с использованием технологий машинного обучения //Вестник УрФО. Безопасность в информационной сфере. – 2021. – №. 4 (42). – С. 39-45.
6. Намиот Д. Е. О кибератаках с помощью систем искусственного интеллекта //Международный журнал открытых информационных технологий. – 2024. – Т. 12. – №. 9. – С. 132-141.
7. Аббасов А.М., Стрельцова Е., Яковенко И., Богомягков А. Математическое моделирование фискальных инноваций на основе междисциплинарного синтеза нечеткой логики и теории автоматов. Азербайджанский математический журнал. - 2022. - Т. 12, Вып. 2. - С. 3-29

8. Стрельцова Е., Бородин А., Яковенко И. Нечетко-логическая модель для обоснования осуществимости проекта: инвестиционный риск проекта. Иранский журнал нечетких систем. – 2022. – Т. 19. – № 2. – С. 1-15.

9. Бородин А., Стрельцова Е., Мамедов З., Яковенко И., Митюшина И. Нечетко-логическая модель анализа устойчивого развития предприятий топливно-энергетического комплекса. АИУС Энергетика. - 2023. - Т. 11, Вып. 5. - С. 974-990

10. Стрельцова Е.Д., Титов А.Ю., Яковенко И.В. Постановка задачи моделирования оценки информационной безопасности. //Друкеровский вестник. - 2024. - № 6. - С. 241-247

11. Стрельцова Е.Д., Титов А.Ю., Яковенко И.В. Математическая модель оценки информационной безопасности хозяйствующих субъектов. //Друкеровский вестник. - 2024. - № 2. - С. 182-193

References

1. Doynikova Ye. V. Model' prognozirovaniya tseley kiberatak na osnove neyronechotkikh setey//Aktual'nyye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2019). – 2019. – S. 405-408.

2. Naumov V. N. i dr. Analiz i prognozirovaniye vremennykh ryadov kiberatak na informatsionnuyu sistemu vedomstvennogo vuza: vozmozhnosti i ogranicheniya metodov //Trudy uchebnykh zavedeniy svyazi. – 2025. – T. 11. – №. 1. – S. 99-112.

3. Mishin A. Ye., Bylevskiy P. G. Primeneniye mashinnogo obucheniya dlya prognozirovaniya kiberatak //Hi-Hume Journal. – 2023. – T. 3. – S. 80.

4. Loshchilin A. V., Yarikov V. G., Nikishova A. V. metody mashinnogo obucheniya v prognozirovanii i predotvrashchenii kiberatak //NBI-technologies. – 2024. – T. 18. – №. 2. – S. 33-39.

5. ASYAYEV G. D., SOKOLOV A. N. Modeli prediktivnoy zashchity informatsii avtomatizirovannoy sistemy upravleniya vodosnabzheniyem na osnove vremennykh ryadov s ispol'zovaniyem tekhnologiy mashinnogo obucheniya //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2021. – №. 4 (42). – S. 39-45.

6. Namiot D. Ye. O kiberatakakh s pomoshch'yu sistem iskusstvennogo intellekta //Mezhdunarodnyy zhurnal otkrytykh informatsionnykh tekhnologiy. – 2024. – T. 12. – №. 9. – S. 132-141.

7. Abbasov A.M., Strel'tsova E., Yakovenko I., Bogomyagkov A. Matematicheskoye modelirovaniye fiskal'nykh innovatsiy na osnove mezhdistsiplinarnogo sinteza nechetkoy logiki i teorii avtomatov. Azerbaydzhanskiy matematicheskiy zhurnal. - 2022. - T. 12, Vyp. 2. - S. 3-29

8. Strel'tsova E., Borodin A., Yakovenko I. Nechetko-logicheskaya model' dlya obosnovaniya osushchestvimosti proyekta: investitsionnyy risk proyekta. Iranskiy zhurnal nechetkikh sistem. – 2022. – T. 19. – № 2. – S. 1-15.

9. Borodin A., Strel'tsova Ye., Mamedov Z., Yakovenko I., Mityushina I. Nechetko-logicheskaya model' analiza ustoychivogo razvitiya predpriyatiy toplivno-energeticheskogo kompleksa. AIUS Energetika. - 2023. - T. 11, Vyp. 5. - S. 974-990

10. Strel'tsova Ye.D., Titov A.YU., Yakovenko I.V. Postanovka zadachi modelirovaniya otsenki informatsionnoy bezopasnosti. //Drukerovskiy vestnik. - 2024. - № 6. - S. 241-247

11. Strel'tsova Ye.D., Titov A.YU., Yakovenko I.V. Matematicheskaya model' otsenki informatsionnoy bezopasnosti khozyaystvuyushchikh sub"yektov. //Drukerovskiy vestnik. - 2024. - № 2. - S. 182-193