Литература

1. Kharin Yu. *Robustness in Statistical Forecasting.* N.Y.: Springer, 2013.
2. Doob J. *Stochastic Processes.* N.Y.: Wiley, 1953.
3. Kharin Yu., Voloshko V. *Robust estimation for Binomial conditionally nonlinear autoregressive time series based on multivariate conditional frequencies* // Journal of Multivariate Analysis. 2021. Vol. 185. P. 11–27.

КОМПЬЮТЕРНЫЙ ПРАКТИКУМ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Харин Ю.С., Мальцев М.В., Гайдук А.Н., Орлов А.А., Палуха В.Ю., Сергеев А.И.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь kharin@bsu.by, maltsew@bsu.com, gaidukan@bsu.com, alex.orlov.official@gmail.com, palukha@bsu.by, giftis95@mail.ru

Информационные технологии стали неотъемлемой частью современного общества. Информация является важнейшим ресурсом, нуждающемся в надежной защите, поэтому специалисты по защите информации требуются каждой компании, заинтересованной в конфиденциальности, целостности и сохранности своих данных. Потребность в таких кадрах обуславливает необходимость качественной подготовки студентов высших учебных заведений по специальностям, связанным с защитой информации. В Белорусском государственном университете ведется подготовка по специальностям 1-98 01 01-01 «Компьютерная безопасность (направление — математические методы и программные системы)», 1-98 01 01-02 «Компьютерная безопасность (направление — радиофизические методы и программно-технические средства)» и 1-97 01 02 «Прикладная криптография». С 2000 года в номенклатуру специальностей научных работников Республики Беларусь включена специальность 05.13.19 «Методы и системы защиты информации. Информационная безопасность». Таким образом, разработка и совершенствование учебных материалов для подготовки специалистов в области защиты информации является актуальной задачей. В 2001 году в Научно исследовательском центре прикладных проблем математики и информатики (в настоящее время — НИИ прикладных проблем математики и информатики) был разработан компьютерный практикум по математическим методам защиты информации [1], предназначенный для практических занятий студентов. С момента выхода практикума появились новые криптографические алгоритмы и протоколы, знание которых необходимо современному квалифицированному IT-специалисту. Кроме того, опыт работы преподавателей специализированных дисциплин показал, что необходимо внести изменения и дополнения в организацию и наполнение практикума.

Разработанный практикум дополняет изданный в Белорусском государственном университете учебник «Криптология» [2] и состоит из следующих составных частей: теоретический материал, задания для лабораторных занятий, выполняемых на компьютере, программная оболочка. Практикум включает в себя такие разделы криптологии, как простейшие («ручные») криптосистемы; генерация и тестирование псевдослучайных последовательностей; алгоритмы шифрования, хэширования, выработки и проверки электронной цифровой подписи; криптографические протоколы. Программная оболочка практикума предназначена для изучения и исследования учащимися криптографических алгоритмов, а также для выполнения заданий практикума. Реализована созможность воздавать криптографические алгоритмы из составных частей (блоки подстановок, перестановок, сумматоры и др.). Программа оснащена удобным интерфейсом, а также имеет архитектуру, позволяющую быстро добавлять новый функционал. Интерфейс программной оболочки практикума представлен на рисунке 1 (реализована сеть Фейстеля).

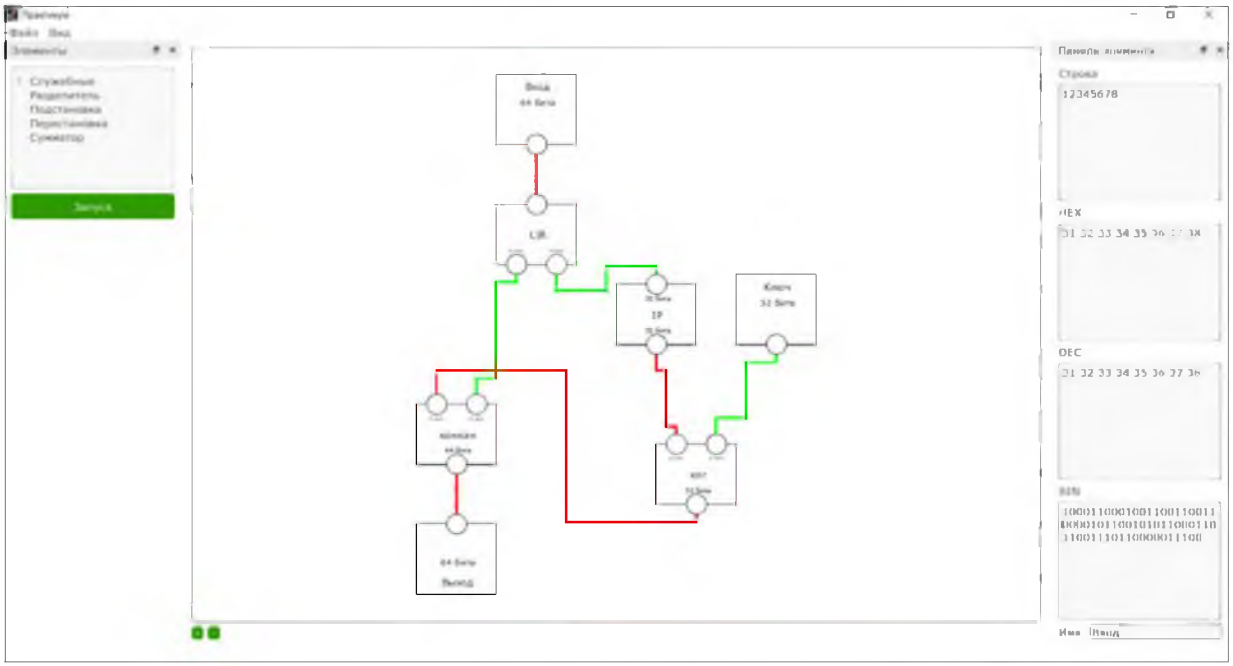

Рис. 1. Интерфейс программной оболочки практикума

Литература

1. Харин Ю.С., Агиевич С.В. *Компьютерный практикум по математическим методам защиты информации: учебное пособие.* Минск: БГУ, 2001.

2. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. *Криптология.* Минск: БГУ, 2014.

ОБ АНАЛИТИЧЕСКИХ ФОРМАХ ПРОИЗВОДСТВЕННЫХ ФУНКЦИЙ ДЛЯ АНАЛИЗА И УЧЕТА НАУЧНО-ТЕХНИЧЕСКОГО ПРОГРЕССА

Г.А. Хацкевич[1], **А.Ф. Проневич**[2]

[1]Институт бизнеса Белорусского государственного университета,
Обойная 7, 220004 Минск, Беларусь Khatskevich@sbmt.by
[2] Гродненский государственный университет имени Янки Купалы,
Ожешко 22, 230023 Гродно, Беларусь pranevich@grsu.by

Долгосрочные тенденции развития экономики любой страны складываются под воздействием многих факторов: характер социальных институтов, отраслевая и воспроизводственная структура народного хозяйства, место и роль страны в системе международных отношений, природные условия и т.д. Однако, начиная с начала XX века на первое место среди этих факторов во всех развитых странах вышел научно-технический прогресс (НТП). Математической базой для анализа и моделирования микро- и макроэкономических процессов, учитывающих НТП, выступает аппарат теории производственных функций (ПФ) [1, 2]:

$$Y = F(K, L, t), \tag{1}$$

где Y — выпуск продукции, K — капитал, L — труд, t — параметр времени из числового луча $\mathbb{R}_+ = [0; +\infty)$, каждое значение которого выражает определенный уровень НТП, а неотрицательная функция F является дважды непрерывно дифференцируемой на множестве $D = G \times \mathbb{R}_+$, экономическая область $G \subset \mathbb{R}^2_+ = \{(K, L) \in \mathbb{R}^2 \colon K \geq 0,\ L \geq 0\}$.

В научной литературе было предложено ряд концепций (см., например, работы [1–5]) к описанию воздействия НТП на экономику и его учета в аналитическом задании ПФ (1). На