

Вопросы науки и образования

№ 26 (38), 2018

Москва
2018





Вопросы науки и образования

№ 26 (38), 2018

НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ
[HTTPS://SCIENTIFICPUBLICATION.RU](https://scientificpublication.ru)
EMAIL: [INFO@SCIENTIFICPUBLICATIONS.RU](mailto:info@scientificpublications.ru)

Главный редактор
КОТЛОВА А.С.

Издается с 2016 года. Выходит 2 раза в месяц
Журнал зарегистрирован Федеральной службой по надзору в сфере связи,
информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство ПИ № ФС77 – 65699

Вы можете свободно делиться (обмениваться) — копировать и распространять материалы и создавать новое, опираясь на эти материалы, с **ОБЯЗАТЕЛЬНЫМ** указанием авторства. Подробнее о правилах цитирования:
<https://creativecommons.org/licenses/by-sa/4.0/deed.ru>

ISSN 2542-081X



Содержание

БИОЛОГИЧЕСКИЕ НАУКИ	6
<i>Абхари Ю.А.</i> НОВЫЙ ВЗГЛЯД НА УВЕЛИЧЕНИЕ КОЛИЧЕСТВА СЕКСУАЛЬНЫХ МЕНЬШИНСТВ.....	6
ГЕОЛОГО-МИНЕРАЛОГИЧЕСКИЕ НАУКИ	9
<i>Мамбетов Ж.С., Медведев К.С.</i> АНАЛИЗ ЭФФЕКТИВНОСТИ МНОГОЗОННОГО ГИДРОРАЗРЫВА ПЛАСТА В УСЛОВИЯХ НИЗКОПРОНИЦАЕМЫХ КОЛЛЕКТОРОВ	9
ТЕХНИЧЕСКИЕ НАУКИ	15
<i>Сбродов Н.Б., Гордеев И.Е.</i> ИССЛЕДОВАНИЕ ПРОЦЕССА НАПЛАВКИ ВНУТРЕННЕГО ПРОХОДА ТРУБОПРОВОДНОЙ АРМАТУРЫ НА ОСНОВЕ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ.....	15
<i>Сидоркин И.И., Маликова М.О., Цуканов М.В.</i> ВЛИЯНИЕ ДИСТОРСИИ КАМЕРЫ НА СШИВАНИЕ ИЗОБРАЖЕНИЙ В ФОТОПЛАН	18
<i>Арзиева Ж.Т.</i> ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И СТОХАСТИЧЕСКИЕ АЛГОРИТМЫ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ.....	20
<i>Филиппова К.Е., Иванов А.А.</i> ВЛИЯНИЕ ЦЕОЛИТСОДЕРЖАЩЕЙ КОМПЛЕКСНОЙ ДОБАВКИ НА ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ	22
<i>Анахин Н.Ю., Грошев Н.Г., Оноприйчук Д.А.</i> СОЛНЕЧНЫЕ БАТАРЕИ – РЕАЛЬНОСТЬ ИЛИ ФАНТАСТИКА?.....	26
<i>Анахин Н.Ю., Грошев Н.Г., Оноприйчук Д.А.</i> BIM ТЕХНОЛОГИИ, КАК ОСНОВА СОВРЕМЕННОГО ОБЪЕКТА.....	29
СЕЛЬСКОХОЗЯЙСТВЕННЫЕ НАУКИ	32
<i>Гузь Ю.Н.</i> ОЦЕНКА УДОВЛЕТВОРЕНИЯ ПИЩЕВЫХ ПОТРЕБНОСТЕЙ КОРЕННЫХ МАЛОЧИСЛЕННЫХ НАРОДОВ СЕВЕРА В МЯСЕ МОРСКИХ МЛЕКОПИТАЮЩИХ.....	32
<i>Гузь Ю.Н.</i> СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ ПРИ ВЕТЕРИНАРНО-САНИТАРНОЙ ЭКСПЕРТИЗЕ МЯСА МОРСКИХ МЛЕКОПИТАЮЩИХ	35
ЭКОНОМИЧЕСКИЕ НАУКИ	37
<i>Говейко С.Н.</i> ТЕХНОЛОГИЯ БЛОКЧЕЙН И РЫНОК НЕДВИЖИМОСТИ.....	37
<i>Товсултанова С.В.</i> К ВОПРОСУ О ФИНАНСОВЫХ ЗАТРАТАХ НА ИННОВАЦИОННЫЙ КОМПЛЕКС ЧЕЧЕНСКОЙ РЕСПУБЛИКИ	38
<i>Аленькина Д.А., Анфиногенова Е.И.</i> НАЛОГОВЫЙ УЧЁТ ЗАТРАТ В КОММЕРЧЕСКИХ ОРГАНИЗАЦИЯХ	41
<i>Сулковский С.В., Петрукович Н.Г.</i> ФИНАНСОВАЯ РАБОТА ОРГАНИЗАЦИИ.....	43
<i>Есмухамбетова С.Ш.</i> ВЛИЯНИЕ ДЕБИТОРСКОЙ ЗАДОЛЖЕННОСТИ НА НАЛОГООБЛОЖЕНИЕ	45

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И СТОХАСТИЧЕСКИЕ АЛГОРИТМЫ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Арзиева Ж.Т.

Арзиева Жамила Тилеубаевна – ассистент,
кафедра прикладной математики,

Каракалтакский Государственный Университет, г. Нукус, Республика Узбекистан

Аннотация: в этой статье рассматриваются задачи генераторов псевдослучайных последовательностей и стохастические алгоритмы защиты информации.

Ключевые слова: псевдослучайных последовательностей (ПСП), компьютерных систем (КС), стеганографический метод, аутентичности, стохастические алгоритмы, криптография, хэш-генератор.

Методы защиты информации, основанные на использовании генераторов псевдослучайных последовательностей (ПСП), будем называть стохастическими. При этом стоит отметить, что иногда термин «стохастические алгоритмы» применяется и в узком смысле тогда, когда речь идет об алгоритмах, предполагающих использование стохастических сумматоров, т.е. сумматоров с непредсказуемым результатом работы, зависящим от заполнения ключевой таблицы. Впервые эти устройства были предложены С.А. Осмоловским и использованы для создания стохастических кодов [1, с. 5].

Можно выделить следующие задачи, требующие решения при построении системы защиты компьютерных систем (КС) ответственного назначения:

1. обеспечение работоспособности компонентов КС и системы в целом при наличии случайных и умышленных деструктивных воздействий;
2. обеспечение секретности информации или наиболее важной ее части;
3. обеспечение аутентичности информации (целостности, подлинности и пр.);
4. обеспечение юридической значимости пересылаемых электронных документов;
5. защита прав собственников информации.

Первая задача решается с применением методов автономного и встроенного диагностирования; контролепригодного и отказоустойчивого проектирования; контроля хода выполнения программ с использованием сторожевых процессоров; помехоустойчивого кодирования; разграничения доступа к ресурсам и компонентам системы; внесения неопределенности в работу средств и объектов защиты.

Вторая задача решается в большой степени криптографическими (шифрование) и в меньшей степени стеганографическими методами (скрытие самого факта хранения или передачи секретной информации).

Третья и четвертая задачи решаются применением криптографических протоколов распределения ключей, аутентификации абонентов, электронной подписи, доказательства с нулевым разглашением знаний и пр.

Решение пятой задачи в настоящее время основано на применении стеганографической технологии цифровых водяных знаков [3, с. 32].

Во всех перечисленных случаях генераторы ПСП применяются либо непосредственно, либо на их основе строятся генераторы случайных последовательностей (СП) и хэш - генераторы (рис. 1). При этом качество защиты в значительной степени определяется качеством используемых алгоритмов генерации ПСП.



Рис. 1. Стохастические алгоритмы в задачах защиты информации

Выводы:

1. Все наиболее эффективные методы защиты информации с полным основанием должны называться стохастическим, так как предполагают прямое или косвенное использование генераторов ПСП.

2. Качество алгоритмов генерации случайных последовательностей и хеширования в первую очередь определяется качеством используемых генераторов ПСП.

3. В этой ситуации возрастает значимость задачи построения эффективных алгоритмов генерации ПСП, а также статистических методов оценки их качества.

Список литературы

1. Осмоловский С.А. Стохастическая информатика. «Радиоэлектроника и управление». № 10-12, 2003.
2. Шеннон К. Математическая теория связи. В сборнике «Работы по теории информации и кибернетике». ИИЛ. Москва, 1963.
3. Осмоловский С.А. Основопологающие работы Шеннона и их использование в современных инфокоммуникациях. // Радиоэлектроника и управление. № 1-3, 2003.