

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

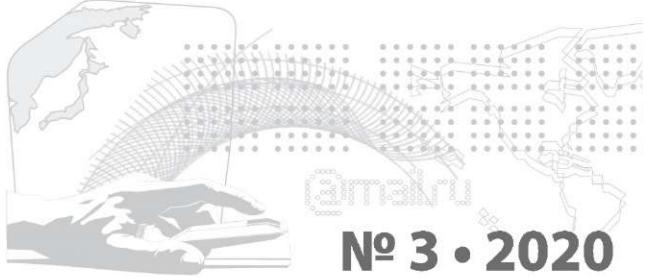
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ

№ 3 • 2020

РАЗДЕЛЫ ВЫПУСКА:

Методы и средства обеспечения информационной безопасности	9
Безопасность распределенных систем и телекоммуникаций	32
Практические аспекты криптографии критические информационные технологии	82
Безопасность программного обеспечения	103
Информационная безопасность киберфизических систем	114



Журнал является органом Совета Регионального Северо-Западного учебно-научного центра информационной безопасности

Журнал включен в перечень изданий, утвержденных ВАК, для публикации основных результатов диссертационных исследований

АДРЕС РЕДКОЛЛЕГИИ:

195251, Санкт-Петербург,
ул. Политехническая, 29.
ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого».

Тел. (812) 552-76-32

e-mail: kafedra@ibks.ftk.spbstu.ru

<http://jisr.ru/kontakty>

Свидетельство о регистрации
№ 018607 от 17.03.99 г. выдано
Государственным комитетом Российской Федерации по печати

С 1 января 2019 г. подписка на журнал «Проблемы информационной безопасности. Компьютерные системы» осуществляется через объединенный каталог «Пресса России»
<https://www.pressa-rf.ru>
Подписной индекс — Т18237

РЕДАКЦИОННЫЙ СОВЕТ:

ВАСИЛЬЕВ Ю. С. — председатель редсовета, акад. РАН, научный руководитель университета, председатель попечительского совета СПбПУ

ЗЕГЖДА П. Д. — главный редактор, д-р техн. наук, проф. кафедры «Информационная безопасность компьютерных систем» СПбПУ

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА:

АБДЫКАППАР АШИМОВ, акад. Национальной академии наук РК, д-р техн. наук, проф., Институт проблем информатики и управления Министерства образования и науки РК, Казахстан;

АТИЛЛА ЭЛЧИ, д-р наук, проф. кафедры «Электроэлектронная инженерия», инженерный факультет, Аксарайский университет, Турция;

БАРАНОВ А. П., д-р физ.-мат. наук, проф., зав. кафедрой «Инновации и бизнес в сфере информационных технологий» НИУ ВШЭ;

БУДЗКО В. И., д-р техн. наук, зам. директора по научной работе Института проблем информатики РАН;

ВЭЙ НЕ, д-р наук, Шенъчженьский университет, Китай;

ГЛУХОВ В. В., д-р экон. наук, проф., первый проректор СПбПУ;

ГРУШО А. А., д-р физ.-мат. наук, проф., зав. кафедрой компьютерной безопасности факультета защиты информации, ГОУ ВПО «Российский государственный гуманитарный университет»;

МОДРИС ГРЕЙТАНС, д-р техн. наук, гл. ред. журн. «Автоматика и вычислительная техника», директор по науке Института электроники и компьютерных наук, Рига, Латвия;

ЕРЕМЕЕВ М. А., д-р техн. наук, проф. кафедры «Системы сбора и обработки информации» ВКА им. А. Ф. Можайского;

ЗЕГЖДА Д. П., д-р техн. наук, проф. РАН, зав. кафедрой «Информационная безопасность компьютерных систем» СПбПУ;

КАЛИНИН М. О., зам. гл. ред., д-р техн. наук, проф. кафедры «Информационная безопасность компьютерных систем» СПбПУ;

КНЯЗЕВ А. В., д-р физ.-мат. наук, проф., генеральный директор АО «Институт точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук»;

КОРНИЕНКО А. А., д-р техн. наук, проф., зав. кафедрой «Информатика и информационная безопасность» ПГУПС;

СИКАРЕВ И. А., д-р техн. наук, проф., зав. кафедрой Морских информационных систем ФГБОУ ВО «Российский государственный гидрометеорологический университет»;

ФРАНК ЛЕПРЕВО, д-р, проф., вице-президент по международным связям Университета Люксембурга;

МАКАРОВ С. Б., д-р техн. наук, проф., директор Института физики, нанотехнологий и телекоммуникаций СПбПУ;

МАЛЮК А. А., канд. техн. наук, проф. кафедры № 41 «Кибербезопасность» НИУ «МИФИ»;

ОСТАПЕНКО А. Г., д-р техн. наук, проф., зав. кафедрой «Системы информационной безопасности» ВГТУ;

РУДСКОЙ А. И., чл.-кор. РАН, д-р техн. наук, проф., ректор СПбПУ;

ВАСИЛЬ СГУРЕВ, акад. Болгарской академии наук, д-р техн. наук, проф., Болгария;

ФЕДОРОВ М. П., акад. РАН, д-р техн. наук, проф., президент СПбПУ;

ХАРИНЮ. С., чл.-кор. НАН Беларуси, д-р физ.-мат. наук, проф., директор НИИ прикладных проблем математики и информатики БГУ;

ЧАНДАН ТИЛАК БХУНИЙ, д-р наук, директор Национального технологического института, Министерство развития человеческих ресурсов Правительства Индии, Аруначал-Прадеш, Индия;

ШЕРЕМЕТ И. А., д-р техн. наук, проф., чл.-кор. РАН, заместитель директора по науке РФФИ;

ШЕЛУПАНОВ А. А., д-р техн. наук, проф., ректор ТУСУР;

ЮСУПОВ Р. М., чл.-кор. РАН, д-р техн. наук, проф., директор СПИИРАН.

Зам. главного редактора **М. О. КАЛИНИН**
Ответственный секретарь **Н. Ю. ЛОВЧИНОВСКАЯ**



МиТСОБИ

29-я конференция

«Методы и технические средства обеспечения безопасности информации»

28 сентября — 1 октября 2020 года

г. Санкт-Петербург, Отель «Parklane resort and Spa»
Крестовский остров, ул. Рюхина 9а.

Конференция «Методы и технические средства обеспечения безопасности информации» (МиТСОБИ) — это встреча профессионалов информационной безопасности, единственная и старейшая конференция, с 1991 года ежегодно проходящая в Санкт-Петербурге.

МиТСОБИ — это возможность узнать самые современные направления и поделиться опытом, это интересные доклады и горячие дискуссии, в которых молодые разработчики имеют возможность узнать мнение мэтров информационной безопасности, а руководители — выяснить, как на практике решать самые острые вопросы, оценить важность и действенность этих решений для обеспечения информационной безопасности как страны в целом, так и для каждого участника киберпространства. Особенность конференции — это диалог на пересечении теории и практики, науки и бизнеса.

Ежегодное количество участников — до 300 человек, среди которых руководство и специалисты органов государственной власти РФ, вузов, академических учреждений, разработчики и молодые ученые, представители научно-исследовательских организаций и коммерческих предприятий из различных регионов России.

Организатор конференции



Соучредители



Комитет
по информатизации
и связи
Правительства
Санкт-Петербурга



Комитет
по науке и высшей
школе
Правительства
Санкт-Петербурга



Санкт-
Петербургский
политехнический
университет
Петра Великого

При участии

Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю, Управления специальной связи и информации ФСО России в СЗФО, Федеральной службы по финансовому мониторингу.

Оргкомитетом конференции за 29 лет работы накоплен огромный опыт по формированию тематик секций, отбору выступающих, проведению круглых столов по актуальным направлениям. В 2020 году планируется обсудить следующие вопросы:

- Кибербезопасность в цифровом мире.
- Безопасность решений на базе блокчейн, криптографические методы и средства защиты информации.
- Интернет вещей и управление безопасностью инфраструктуры.
- Big Data в задачах информационной безопасности.
- Подготовка специалистов в области информационной безопасности.
- Вопросы информационной безопасности: взгляд молодых ученых.

Тезисы докладов участников конференции публикуются в ежегодном сборнике, который индексируется РИНЦ. Лучшие доклады могут быть опубликованы в журнале Automatic Control and Computer Sciences издательства Allerton Press, который индексируется Scopus. Все участники конференции получают сертификаты о прохождении обучения, согласованные с Учебно-методическим объединением по информационной безопасности.

Конференция МиТСОБИ-2020 пройдет в самом центре Санкт-Петербурга, на Крестовском острове, в комфортабельном SPA-отеле Parklane. Отель находится на территории Приморского парка Победы, среди аллей вековых деревьев, в двух шагах от Финского залива. Здесь есть все преимущества загородного отдыха в самом сердце мегаполиса, в пешей доступности от станции метро «Крестовский остров».

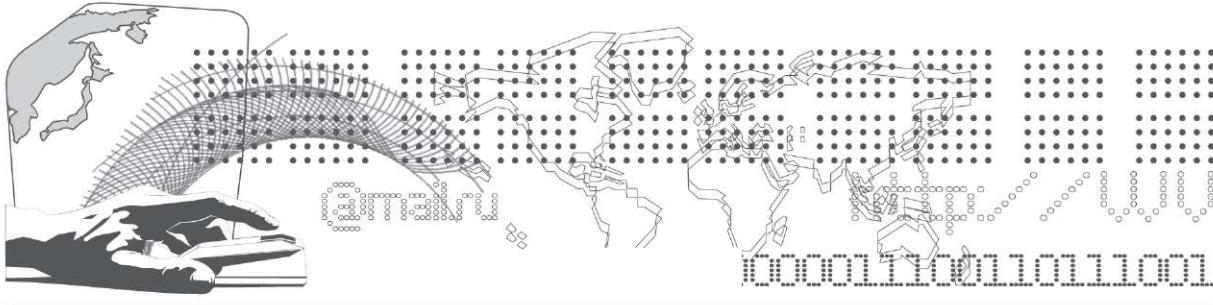
В рамках конференции пройдет NeoQUEST-2020 — это ежегодное испытание для специалистов в области кибербезопасности, участники которого решают увлекательные задачи, взятые из практики обеспечения безопасности современных информационных технологий. Блокчейн и постквантовая криптография, Deep Learning в задачах ИБ, тестирование на проникновение, безопасность современных автомобилей — эти и многие другие темы будут обсуждаться на NeoQUEST. Гости NeoQUEST смогут поучаствовать в воркшопах и мастер-классах, обучающих работе с самыми современными технологиями защиты; в режиме реального времени пройдут демонстрации наиболее значимых современных кибератак и способов защиты от них.

Подробная информация — на сайте конференции www.mitsobi.ru.

Контактные лица:

**Селиванова Анна Юрьевна — 8 (800) 222-28-06 (звонок бесплатный);
+7 (812) 535-28-06.**

E-mail: mitsobi@neobit.ru.



СОДЕРЖАНИЕ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 9 Грушо Н. А., Грушо А. А., Тимонина Е. Е.**
ЛОКАЛИЗАЦИЯ СБОЕВ С ПОМОЩЬЮ МЕТАДАННЫХ
- 16 Лось В. П., Никульчев Е. В., Пушкин П. Ю., Русаков А. М.**
**ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА
МОНИТОРИНГА ВЫПОЛНЕНИЯ ОПЕРАТОРАМИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА**
- 24 Антонов Р. А., Карабанская Е. В., Хандожко Г. В.**
**ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ
ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ
УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИЙ

- 32 Мясников А. В.**
**ПОСТРОЕНИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ
ДЛЯ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ**
- 40 Еремеев М. А., Нефедов В. С., Островский А. С., Семченков Д. А.**
**ПОДХОД К ОБНАРУЖЕНИЮ СКРЫТЫХ КАНАЛОВ
В DNS-ТРАФИКЕ ПУТЕМ ВЫЯВЛЕНИЯ СИГНАЛОВ-МАЯКОВ**
- 50 Калинин М. О., Крундышев В. М., Синяпкин Б. Г.**
**РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ
В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ АЛГОРИТМА
ВЫРАВНИВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ**
- 59 Алексеев И. В., Зегжда П. Д.**
**АДАПТИВНЫЙ МЕХАНИЗМ ОБНАРУЖЕНИЯ РАСПРЕДЕЛЁННЫХ АТАК ОТКАЗА
В ОБСЛУЖИВАНИИ В КРУПНОМАСШТАБНЫХ СЕТЯХ**

ПРАКТИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ

- 65 Алексеев Е. К., Ахметзянова Л. Р., Николаев В. Д., Смышиляев С. В., Бондаренко А. И.**
О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ ПРОТОКОЛА NB-FI

- 74** Бабаш А. В.
ДЕШИФРОВАНИЕ ШИФРА СЛУЧАЙНОГО ГАММИРОВАНИЯ

КРИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

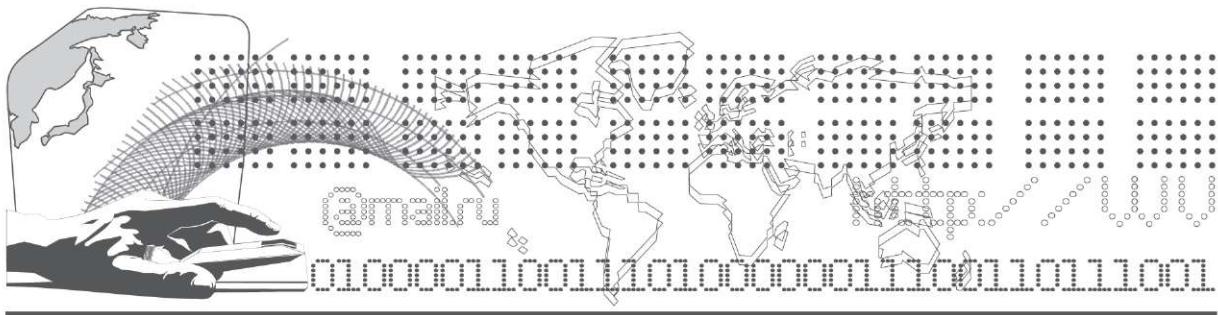
- 82** Горбачёв И. Е., Криулин А. А., Латыпов И. Т.
МЕТОДИКА МЕДИАМЕТРИЧЕСКОГО АНАЛИЗА ИНФОРМАЦИИ
С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ
- 92** Макаров А. С.
ВРЕМЕННАЯ АТАКА НА ПРИМЕРЕ МИКРОКОНТРОЛЛЕРА AVR
- 97** Сухопаров М. Е., Лебедев И. С., Семенов В. В.
АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
МОБИЛЬНЫХ ОБЪЕКТОВ ТРАНСПОРТНЫХ СИСТЕМ

БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- 103** Овасапян Т. Д., Князев П. В., Москвин Д. А.
АВТОМАТИЗИРОВАННЫЙ ПОИСК УЯЗВИМОСТЕЙ В ПРОГРАММНОМ
ОБЕСПЕЧЕНИИ АРХИТЕКТУРЫ ARM С ПРИМЕНЕНИЕМ
ДИНАМИЧЕСКОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

- 114** Фатин А. Д., Павленко Е. Ю.
АНАЛИЗ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ
- 123** Дахнович А. Д., Москвин Д. А., Зегжда Д. П.
ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ КИБЕРУСТОЙЧИВОСТИ
ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ



CONTENTS

INFORMATION SECURITY APPLICATION

- 9 Grusho N. A., Grusho A. A., Timonina E. E.**
LOCALIZING FAILURES WITH METADATA
- 16 Los V. P., Nikulchev E. V., Pushkin P. Yu., Rusakov A. M.**
**INFORMATION-ANALYTICAL SYSTEM OF MONITORING IMPLEMENTATION
OF LEGISLATION REQUIREMENTS BY PERSONAL INFORMATION OPERATORS**
- 24 Antonov R. A., Karachanskaya E. V., Khandozhko G. V.**
**USING ARTIFICIAL NEURAL NETWORKS TO DETERMINE PROBABILITY
OF INFORMATION SECURITY THREATS**

NETWORK AND TELECOMMUNICATION SECURITY

- 32 Myasnikov A. V.**
**BUILDING INFORMATION SYSTEM MODEL FOR APPLICATION
IN PENETRATION TESTING AUTOMATION PROBLEM**
- 40 Eremeev M. A., Nefedov V. S., Ostrovsky A. S., Semchenkov D. A.**
**APPROACH TO DETECT DNS-BASED COVERT CHANNELS
BY IDENTIFYING BEACON SIGNALS**
- 50 Kalinin M. O., Krundyshev V. M., Sinyapkin B. G.**
**DEVELOPMENT OF INTRUSION DETECTION SYSTEM
IN INTERNET OF THINGS NETWORK BASED
ON SEQUENCE ALIGNMENT ALGORITHM**
- 59 Alekseev I. V., Zegzhda P. D.**
**ADAPTIVE MECHANISM FOR DETECTING DISTRIBUTED DENIAL
OF SERVICE ATTACKS IN LARGE-SCALE NETWORKS**

APPLIED CRYPTOGRAPHY

- 65 Alekseev E. K., Akhmetzyanova L. R., Nikolaev V. D., Smyshlyayev S. V., Bondarenko A. I.**
ON CRYPTOGRAPHIC PROPERTIES OF NB-FI PROTOCOL
- 74 Babash A. V.**
ATTACKS FOR ONE-TIME PADS

SPECIAL IT

- 82** *Gorbachev I. E., Kriulin A. A., Latipov I. T.*
**METHODS OF MEDIAMETRIC ANALYSIS OF INFORMATION
USING MACHINE LEARNING ALGORITHMS**

- 92** *Makarov A. S.*
TIME ATTACK ON EXAMPLE OF AVR MICROCONTROLLER

- 97** *Sukhoparov M. E., Lebedev I. S., Semenov V. V.*
**ANALYSIS OF STATE OF INFORMATION SECURITY OF MOBILE OBJECTS
OF TRANSPORT SYSTEMS**

SOFTWARE SECURITY

- 103** *Ovasapyan T. D., Knyazev P. V., Moskvin D. A.*
**AUTOMATED VULNERABILITY SEARCH IN ARM ARCHITECTURE SOFTWARE
USING DYNAMIC SYMBOLIC EXECUTION**

INFORMATION SECURITY CYBER-PHYSIC SYSTEMS

- 114** *Fatin A. D., Pavlenko E. Yu.*
**ANALYSIS OF APPROACHES TO ENSURING
INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS**

- 123** *Dakhnovich A. D., Moskvin D. A., Zegzhda D. P.*
INDUSTRIAL INTERNET OF THINGS CYBER-RESILIENCE REQUIREMENTS

УДК 003.26

A. V. Бабаш

Москва, Российский экономический университет им. Плеханова
Москва, Национальный исследовательский университет «Высшая школа экономики»

ДЕШИФРОВАНИЕ ШИФРА СЛУЧАЙНОГО ГАММИРОВАНИЯ

Представлены две атаки на шифр случайного гаммирования с расчетом трудоемкости и надежности.

Ключевые слова: шифр случайного гаммирования, трудоемкость криптографического метода, надежность криптографического метода

A. V. Babash

ATTACKS FOR ONE-TIME PADS

Two attacks on the random gamma code are given with the calculation of the complexity and reliability.

Keywords: Random Gamma Code, Complexity of the Cryptographic Method, Reliability of the Cryptographic Method

Понятие совершенного шифра впервые появилось в статье [1], а первоисточником понятия «совершенной секретности» для советских специалистов стала книга Клода Шеннона [2]. В этой книге понятие совершенной секретности шифра К. Шеннон объяснил с помощью следующего условия: «Для всех криптограмм апостериорные вероятности равны априорным вероятностям независимо от величины последних. В этом случае перехват сообщения не дает шифровальщику противника никакой информации. Теперь он не может корректировать никакие свои действия в зависимости от информации, содержащейся в криптограмме, так как все вероятности, относящиеся к содержанию криптограммы, не изменяются. С другой стороны, если это условие равенства вероятностей не выполнено, то имеются такие случаи, в которых для определенного ключа и определенных выборов сообщений апостериорные вероятности противника отличаются от априорных. Это, в свою очередь, может повлиять на выбор противником своих действий и, таким образом, совершенной секретности не получится».

Российские криптографы трактуют понятие совершенно секретного шифра как шифра, совершенного по К. Шеннону, и называют такие шифры теоретически стойкими, понимая под этими названиями шифры, которые не поддаются дешифрованию по известному шифрованному тексту. Примером такого шифра как в российских учебниках, так и в зарубежных выступает шифр случайного гаммирования и его частный случай — шифр Вернама.

Приводится обоснование дешифруемости шифра случайного гаммирования (ШСГ). Приводятся две атаки определения открытого текста по известному шифрованному тексту ШСГ с расчетом параметров их сложности.

1. Модель шифра К. Шеннона и описание ШСГ

Для описания ШСГ нам потребуется вероятностная модель шифра К. Шеннона. С этой целью введем следующие обозначения: X — конечное множество, состоящее из двух или более элементов и названное множеством открытых текстов; K — конечное множество, состоящее из

двух или более элементов и названное множеством ключей; Y — конечное множество, состоящее из двух или более элементов и названное множеством шифрованных текстов; $(f_k)_{k \in K}$ — семейство инъективных отображений $X \rightarrow Y$; $f_k(x) = y$ — уравнение шифрования $x \in X$, $y \in Y$; $(f_k^{-1})_{k \in K}$ — обратные к $(f_k)_{k \in K}$ отображения, если $f_k(x) = y$, то $f_k^{-1}(y) = x$; $f_k^{-1}(y) = x$ — уравнение расшифрования; $f: X \times K \rightarrow Y$ — сюръективное отображение, $f(x, k) = f_k(x)$; M — подмножество множества X , названное множеством содержательных текстов, которые имеют некоторую «структуру», позволяющую отличить элемент x из M от элемента из $X \setminus M$ с некоторой надежностью.

Например, $X = I^L$ состоит из конечных слов $x = i_1 i_2 \dots i_L$ в алфавите I длины L некоторого естественного языка, а M из читаемых последовательностей вида $m = i_1 i_2 \dots i_L$, то есть имеющих некоторое содержание.

$P(M) = (p(m), m \in M)$ — дискретное вероятностное распределение на множестве M ; $P(K) = (p(k), k \in K)$ — дискретное вероятностное распределение на множестве K .

Определение 1. Пятерку введенных объектов:

$$(M, K, C, (f_k)_{k \in K}, (f_k^{-1})_{k \in K}) \\ P(M), P(K))$$

назовем вероятностной моделью шифра (схемы шифрования) Клода Шеннона. Кратко — модель шифра.

Вероятностные распределения $P(M)$, $P(K)$ индуцируют: вероятностное распределение $P(Y) = (p(y), y \in Y)$ на множестве Y ; условное вероятностное распределение $P(M|y) = (p(m|y), m \in M)$ для каждого $y \in Y$; условное вероятностное распределение $P(Y|m) = (p(y|m), y \in Y)$ для каждого $m \in M$; условное вероятностное распределение $P(K|y) = (p(k|y), k \in K)$ для каждого $y \in Y$; условное вероятностное распределение $P(Y|k) = (p(y|k), y \in Y)$ для каждого $k \in K$.

Определение 2. Шифр считается совершенным по К. Шенону [3], если для каждого распределения вероятностей на множестве M для каждого сообщения

$m \in M$ и каждого зашифрованного текста $y \in Y$ (для которого вероятность $(p(y) > 0)$ выполняется равенство:

$$p(m|y) = p(m).$$

Требование $p(y) > 0$ техническое, оно необходимо для предотвращения использования события с нулевой вероятностью.

Перейдем к описанию шифра случайного гаммирования. Его можно найти во многих российских и зарубежных источниках. Обозначим через $I = \{0, 1, \dots, n - 1\}$ номера упорядоченного алфавита используемого естественного языка. Пусть $X = K = Y = I^L$ и подмножество $M \subseteq X$ есть множество содержательных текстов длины L . Для шифрования открытого содержательного текста буквы текста кодируются своими номерами. При расшифровании номера шифрованного текста декодируются в буквы. Для $x = i_1 i_2 \dots i_L \in M$ и $k = \gamma_1 \gamma_2 \dots \gamma_L \in K$ уравнение шифрования $f(x, k) = y$ имеет вид $i_j + \gamma_j = y_j \bmod n, j \in \{1, \dots, L\}$ $y = y_1 y_2 \dots y_L \in Y$. Уравнение расшифрования имеет вид $y_j - \gamma_j + n = i_j \bmod n, j \in \{1, \dots, L\}$. Предполагается, что ключи выбираются случайно, равновероятно и независимо от открытого текста. В учебниках по криптографии доказано, что ШСГ является совершенным.

2. Утверждения о недешифруемости ШСГ

Авторы многих источников утверждают, что ШСГ недешифруемы. Приведем частично их утверждения.

«In this chapter, we look at the other extreme and study encryption schemes that are provably secure even against an adversary who has unbounded computational power. Such schemes are called perfectly secret» [3, p. 35].

«The hotline between the United States and the former Soviet Union was (is it still active?) rumored to be encrypted with a one-time pad. Many Soviet spy messages to agents were encrypted using one-time pads. These messages are still secure today and will remain that way forever. It doesn't matter how long the supercomputers work on the problem. Even after the aliens from Andromeda land with their massive spaceships and undreamed-of

computing power, they will not be able to read the Soviet spy messages encrypted with one-time pads (unless they can also go back in time and get the one-time pads) [4, p. 26].

«При рассмотрении вопроса о теоретической стойкости шифров отвлекаются от реальных временных и сложностных затрат по вскрытию шифра (что определяет подход к практической стойкости). Во главу угла ставится принципиальная возможность получения некоторой информации об открытом тексте или использованном ключе. Впервые такой подход исследовал К. Шенон. Он рассматривал уже знакомую нам модель шифра и единственную криптоатаку на основе шифртекста. Проследим за его рассуждениями. Как мы указывали, конечной целью работы криptoаналитика является текст сообщения или ключ шифрования. Однако весьма полезной может быть даже некоторая вероятностная информация об открытом тексте. Например, уже предположение о том, что открытый текст написан по-английски, представляет криptoаналитику определенную априорную информацию об этом сообщении даже до того, как он увидит шифртекст» [5, стр. 172].

Математическое обоснование недешифруемости ШСГ состоит в следующем. Рассмотрим уравнение шифрования ШСГ $i_j + \gamma_j = y_j \text{ mod } n$, $j \in \{1, \dots, L\}$, $y = y_1y_2\dots y_L \in Y$. При фиксированном $y = y_1y_2\dots y_L \in Y$ для каждого символа i_j существует единственный символ ключа γ_j , при котором справедливы указанные равенства. Ключ $k = y_1y_2\dots y_L \in K$ выбирался равновероятно. Следовательно, каждый открытый текст мог со своей априорной вероятностью быть решением данной системы уравнений. Поэтому определить открытый текст не представляется возможным.

3. Краткий обзор предварительных результатов

В работах [6–8] было доказано, что мнение о недешифруемости совершенных шифров ошибочно. Доказательство было основано на уточнениях понятия совершенности шифра, представленных в [9]. Именно дан-

ное выше определение ([3, стр. 32]) подразумевает атаки на открытый текст $t \in M$ по известному шифрованному тексту $u \in Y$. Аналог же определения совершенности шифра по атакам на ключ $k \in K$ по известному шифрованному тексту $u \in Y$ выглядит так: $p(k/u) = p(k)$ при любых $k \in K$ и $u \in Y$ [9]. Это условие выполняется не всегда: оно не выполняется для шифра случайного гаммирования, так как $p(k/u) = p(m)$ при m , для которого $f_k(m) = u$. Из результатов [6–8] следует, что шифр случайного гаммирования можно дешифровать. Описание предполагаемых атак было дано в [10]. Приводимые ниже атаки на ШСГ будут основаны на известных идеях методов дешифрования шифра Виженера.

Определение 3. Ключ $k = \gamma_1\gamma_2\dots\gamma_L$ ШСГ длины $L = qd + r$, $r < d$ называется d -слабым (имеет локальный периодом d , [9]), если его d -граммы

$$\begin{aligned} &\gamma_{vd+1}\gamma_{vd+2}\dots\gamma_{(v+1)d}, \\ &v \in \{0, 1, d+1, \dots, (q-1)d\} \end{aligned}$$

одинаковы и $q \geq 2$.

Необходимо учитывать, что d -слабый ключ при $L = qd + r$, $r < d$ является одновременно и wd -слабым ключом при $2w \leq q$.

4. Описание Шифра Виженера и его дешифрование

Шифр, который известен под именем Виженера [11, 12–17], впервые описал Джованни Баттиста Беллазо (Giovanni Battista Bellaso) в своей книге «La cifra del Sig. Giovan Battista Belaso». Часто этот шифр называют «лозунговым шифром», или «шифром с короткой периодической гаммой». Краткое описание такого шифра состоит в следующем. В множестве d -слабых ключей $d \in \left\{2, 3, \dots, \left[\frac{L}{2}\right]\right\}$ шифра случайного гаммирования выделим d -слабые ключи минимальной длины. Шифр Виженера получается из ШСГ, если для шифрования открытых текстов выбирать только минимальные d -слабые ключи, называемые «лозунгами» длины d , $d \in \left\{2, 3, \dots, \left[\frac{L}{2}\right]\right\}$. Процесс шифрования и расшифрования остается таким же, как и в ШСГ.

Атаки на шифр Виженера широко известны специалистам по криптографии. Эти атаки с примерами его дешифрования можно найти в [9]. Все атаки состоят из двух этапов. Первый этап состоит в определении по известному шифрованному тексту длины лозунга, то есть значения d в использованном минимальном d -слабом ключе. Эта задача решается двумя методами.

Метод Фридриха Казисского, представленный в 1863 году, анализирует повторения в шифртексте для шифра Виженера. Этот же метод независимо от Казисского был разработан советским криптографом Михаилом Соколовым. Данный метод широко известен в криптографической литературе. Метод основан на том, что если ключ периодический, то две одинаковые m -граммы открытого текста, отстоящие друг от друга на расстоянии, которое кратно периоду ключа, будут одинаково зашифрованы в некоторые одинаковые m -граммы, находящиеся на том же расстоянии друг от друга. Появление же одинаковых m -грамм в шифрованном тексте по другим причинам маловероятно (при некоторых разумных ограничениях на величину m и на длину шифртекста N). Следовательно, большинство расстояний (т. е., возможно, не все) между одинаковыми m -граммами шифртекста делятся на минимальный период d . Поэтому на практике в качестве предполагаемой длины лозунга в шифре Виженера рассматривают наибольший общий делитель длин большинства расстояний между повторениями m -грамм. Эксперименты для английского языка показали хорошую надежность этого метода, если в шифртексте имеются повторения триграмм и m -грамм при $m=3$ и большим трех [5].

Уильям Фредерик Фридман в 1920 году опубликовал результаты своих научных исследований по дешифрованию шифра Виженера [11]. Метод основывался на том, что если взять элементы шифрованного текста шифра Виженера, выбранные с шагом выборки равным длине лозунга, и рассчитать вероятность совпадения выбранных эле-

ментов на случайно и равновероятно выбранных местах, то эта вероятность будет приблизительно равна $\sum_{i \in I} p_i^2$, где p_i — вероятность появления буквы i в открытых текстах.

Второй этап атак на шифр Виженера состоит в определении двух открытых текстов, зашифрованных одним ключом. Дело в том, что на первом этапе было определено значение d (d -слабого ключа $k = \gamma_1\gamma_2\dots\gamma_L$). Следовательно, ключ можно представить в виде $k = \gamma_1\gamma_2\dots\gamma_{qd}\dots\gamma_{qd+r}$ с повторяющимися q раз отрезками ключа длины d . Поэтому неизвестный открытый текст $x = i_1i_2\dots i_{qd+r}$ задает неизвестные тексты $x(1) = i_{d+1}i_{d+2}\dots i_{(q-1)d}$ и $x(2) = i_{d+1}i_{d+2}\dots i_{qd}$, зашифрованные одним ключом $k = \gamma_1\gamma_2\dots\gamma_{qd}\dots\gamma_{qd}$. Методы определения этих двух текстов широко известны. Они работают с малой трудоемкостью. Один из них называется «методом протяжки вероятного слова». В более общей ситуации, а именно в задаче дешифрования шифра поточной замены при известном периоде ключевой последовательности этот метод подробно изложен в [9, стр. 180]. Обычно этот метод широко используют в учебных целях. Второй метод называется «Метод одновременного зигзагообразного чтения двух открытых текстов в колонках» [9, стр. 180–185]. Ниже мы используем его при дешифровании двух открытых текстов: $x(1) = i_1i_2\dots i_{(q-1)d}$ и $x(2) = i_{d+1}i_{d+2}\dots i_{qd}$, зашифрованных на одном ключе единственным ключом $\gamma_1\gamma_2\dots\gamma_{(q-1)d}$. Для удобства назовем этот метод *основным* и дадим его краткое описание. Из законов функционирования шифра Виженера вытекают следующие следствия:

$$i_j - i_{d+j} = y_j - y_{d+j} \pmod{n}, \\ j \in \{1, 2, \dots, (q-1)d\}.$$

Правые части $\Delta_j = y_j - y_{d+j} \pmod{n}$, $j \in \{1, 2, \dots, (q-1)d\}$ уравнений известны, поэтому число возможных пар (i_j, i_{d+j}) в каждой левой части каждого j -того уравнения равно $|I|$. Каждому открытому тексту $x(1) = i_1i_2\dots i_{(q-1)d}$ соответствует единственный открытый текст $x(2) = i_{d+1}i_{d+2}\dots i_{qd}$. На этом свойстве основан метод одновременного

зигзагообразного чтения открытых текстов в колонках. В более общей ситуации он детально изложен в [9, стр. 181]. Практика дешифрования шифра Виженера методом одновременного зигзагообразного чтения двух открытых текстов в колонках показала, что при значении d таком, что открытые тексты длины d распознаются (читаются) в множестве $|I|^d$, ложные решения отсутствуют. Дополнительным обоснованием этого можно считать наличие общей части $i_{d+1}i_{d+2}\dots i_{(q-1)d}$ в двух открытых текстах. Имеет место важный исторический факт: «Интересным примером этого является проект VENONA, в рамках которого США и Великобритания смогли расшифровать зашифрованные тексты, посланные Советским Союзом, которые ошибочно зашифровывали сообщения повторяющимися ключами с помощью одноразового блокнота» [3, стр. 34]. Таким образом, подтверждено практическое дешифрование двух открытых текстов, зашифрованных одним ключом ШСГ.

5. Критерии определения d -слабого ключа ШСГ

Пусть $y = y_1y_2\dots y_L$ шифрованный текст ШСГ, полученный при шифровании открытого текста $x = i_1i_2\dots i_L \in M$ при случайно и равновероятно выбранном ключе $k = \gamma_1\gamma_2\dots\gamma_L \in K$. Без ограничения общности считаем, что $L = qd$, $q > 1$. В атаках на ШСГ мы будем пользоваться следующими критериями, вытекающими из изложенного выше первого этапа дешифрования Шифра Виженера.

Ниже будем считать, что на I задано вероятностное распределение $(p_i, i \in I)$.

Критерий d -слабого ключа (критерий Фридмана). Ключ k d -слабый тогда и только тогда, когда при каждом j из $\{1, 2, \dots, d\}$ для последовательности $y_jy_{j+d}, y_{j+2d}, \dots$ выполняется приближенное равенство

$$\sum_{i \in I} \frac{v_i(v_i - 1)}{q(q-1)} \approx \sum_{i \in I} p_i^2, \quad (1)$$

где v_i — частота символа $i \in I$ в последовательности $y_jy_{j+d}y_{j+2d}\dots y_{j+(q-1)d}$.

Для d -слабого ключа предел левой части (1) при $q \rightarrow \infty$ равен правой части (1). Более точные выражения даны в [9, стр. 156]. Естественно, надежность $P(L, d)$ таких критериев возрастает с ростом L , а также с уменьшением d . Рекомендуется использовать критерии 1 при больших значениях q .

Критерий d -слабого ключа (критерий Казисского). Ключ k wd -слабый, $w < 2q$ тогда и только тогда, когда наибольший общий делитель длин большинства расстояний между повторениями 3-грамм и m -грамм при $m > 3$ равен d . Рекомендуем использовать при больших значениях L .

Далее предполагается, что критерии 1–2 работают с надежностью 1.

6. Атаки на шифр случайного гаммирования

Обозначим через $M(d)$ множество всех отрезков длины d открытых текстов из M . Минимальное d , при котором открытый текст $i_1i_2\dots i_d$ распознается (читается) в множестве $|I|^d$, назовем расстоянием распознаваемости открытого текста и обозначим его через d^* .

Атака 1. Без ограничения общности считаем, что $L = qd$, $d \geq d^*$ и пара (L, d) такова, что $P(L, d) \gg 1$ для критериев 1, 2. Проверяем по одному из этих критериев, является ли использованный ключ d -слабым ключом. Если нет, то атака завершена неуспешно. Если да, то реализуем основной метод дешифрования шифрованных текстов, полученных из двух открытых текстов, зашифрованных одним ключом. Атака завершена успешно.

Вероятность использования шифровальщиком d -слабого ключа рана:

$$\frac{|I|^d}{|I|^L}.$$

Следовательно, надежность метода равна:

$$\frac{P(L, d)}{|I|^{L-d}} \approx \frac{1}{|I|^{L-d}}.$$

Трудоемкость атаки 1 с фиксированным параметром d определяется реали-

зацией критерия на определение использования d-слабого ключа, которую будем считать за одну операцию, и дополнительно определяется еще одной операцией в случае положительного решения об использовании при шифровании d-слабого ключа, именно операции определения двух открытых текстов, зашифрованных единственным ключом. Следовательно, трудоемкость атаки 1 равна:

$$\left(1 - \frac{1}{|I|^{L-d}}\right) + 2 \frac{1}{|I|^{L-d}} \approx \frac{2}{|I|^{L-d}}.$$

Атака 2. Пусть $d \geq d^*$ и $L = qd$. Опробуем все ключи $k_d \in I^d$.

1. На каждом опробуемом ключе k_d расшифровываем первую d-граммму $y_1y_2...y_d$ шифрованного текста $y = y_1y_2...y_L$ с целью построения множества всех пар $(x(t), k(x(t)))$. Здесь $k(x(t))$ ключ из I^d , расшифровывающий шифрованный текст $y_1y_2...y_d$ в некоторый открытый текст $x(t) \in M(d)$. Множество всех ключей $k(x(t))$ обозначим через $K(M(d))$. Для построения множества всех пар $(x(t), k(x(t)))$ требуется выполнить $|I|^d$ операций опробований ключей.

2. Последовательно расшифровываем вторую d-граммму $y_{d+1}y_{d+2}...y_{2d}$ шифрованного текста $y = y_1y_2...y_L$ на каждом ключе $k(x(t))$ из $K(M(d))$ с целью получения какого либо текста $x(j)$ из $M(d)$. Число таких операций равно $|K(M(d))| = |M(d)|$. Возможно два случая:

1) При каждом ключе $k(x(t))$ из $K(M(d))$ открытый текст не получен, в этом случае использованный ключ шифра не является d-слабым, атака завершена неудачно. Затраченная трудоемкость равна:

$$\left(|I|^d + |M(d)|\right) \left(1 - \frac{1}{|I|^d}\right).$$

2) На одном из ключей $k(x(t))$ получен открытый текст $x(j)$ из $M(d)$. Следовательно, мы дешифровали первые две d-граммы шифрованного текста конкатенацией ключей $k(x(t))k(x(t))$ и получили открытый текст — конкатенацию $x(t)x(j)$. В случае $q = 2$ атака завершена удачно. Затраченная трудоемкость равна:

$$\left(|I|^d + |M(d)|\right) \frac{1}{|I|^d}.$$

Общая трудоемкость атаки при $q = 2$ равна:

$$|I|^{\frac{L}{2}} + \left|M\left(\frac{L}{2}\right)\right|.$$

Ее надежность равна вероятности $\frac{1}{|I|^{\frac{L}{2}}}$

использования шифровальщиком $\frac{L}{2}$ -слабого ключа.

В случае $q \geq 3$ при условии расшифрования первых двух d-грамм проверяем, расшифровывает ли ключ $k(x(t))$ остальные $q-2$ d-граммы шифрованного текста в открытые тексты. Трудоемкость этой проверки равна не больше $q-2$. Если ключ $k(x(t))$ расшифровывает, то использованный при шифровании ключ d-слабый и одновременно мы нашли весь открытый текст. В противном случае ключ не является d-слабым. В обоих случаях атака завершена.

Надежность атаки равна вероятности $\frac{1}{|I|^{L-d}}$ использования шифровальщиком d-слабого ключа. Трудоемкость атаки при $q \geq 3$ равна:

$$\left(|I|^d + |M(d)| + q - 2\right) \frac{1}{|I|^{L-d}}$$

в случае ее успешного завершения. В противном случае трудоемкость атаки не больше величины:

$$\left(|I|^d + |M(d)| + q - 2\right) \left(1 - \frac{1}{|I|^{L-d}}\right);$$

Следовательно, общая трудоемкость атаки не больше:

$$\left(|I|^d + |M(d)| + q - 2\right).$$

Замечание к атаке 2. Ниже приводятся три математических модели в обосновании единственности конкатенации $x(t)x(j)$ в случае использования d-слабого ключа.

Модель 1. Предположим противное. Получили две пары конкатенаций x^1x^2, x^3x^4 открытых текстов $x^1 = i_1^{1,1} \dots i_d^{1,d}$, $x^2 = i_{d+1}^{1,1} i_{d+2}^{1,2} \dots i_{2d}^{1,d}$ и $x^3 = i_1^{2,1} i_2^{2,2} \dots i_d^{2,d}$, $x^4 = i_{d+1}^{2,1} i_{d+2}^{2,2} \dots i_{2d}^{2,d}$. Следствием наличия таких пар согласно законам функционирования ШСГ являются две системы равенств:

$$\begin{aligned} i_j^1 - i_{j+d}^1 &= y_j - y_{j+d} \bmod n, \quad j \in \{1, 2, \dots, d\}, \\ i_j^2 - i_{j+d}^2 &= y_j - y_{j+d} \bmod n, \quad j \in \{1, 2, \dots, d\}. \end{aligned}$$

Следовательно, справедливы равенства:

$$i_j^1 - i_{j+d}^1 = i_j^2 - i_{j+d}^2 \bmod n, \quad j \in \{1, 2, \dots, d\}. \quad (3)$$

Естественно считать, что если две пары открытых текстов выбраны случайно и равновероятно из множества $M(d) \times M(d)$, то вероятность события (3) равна $\frac{1}{|I|^d}$. Значит, вероятность получения двух пар конкатенаций открытых текстов не больше $\frac{1}{|I|^d}$. Поэтому вероятность единственности полученной конкатенации $x(i)x(j)$ больше $1 - \frac{1}{|I|^d}$. Данный факт обосновывает предположение, что полученная конкатенация $x(i)x(j)$ единственная.

Модель 2. Согласно результатам К. Шеннона [1, 2] число открытых (содержательных) текстов длины N равно приблизительно 2^{HN} , где H энтропия на букву сообщения. Для русского и английского языков считают, что $H = 1$. Положив, для примера, $|I| = 32$, имеем $\frac{|I|^N}{2^{HN}} = \frac{2^{5N}}{2^N} = 2^{4N}$, что говорит о том, что мощность $M(N)$ открытых текстов, как правило, много меньше числа $|I|^N$. Будем считать, что множество ключей $K(M(d))$ получено случайной и равновероятной выборкой из $|I|^N$.

Тогда при расшифровании шифрованного текста длины d на каждом ключе k из $K(M(d))$ среднее число получаемых открытых текстов равно $\frac{|M(d)|^2}{|I|^d}$. В случае, когда $|M(d)| \leq |I|^{\frac{d}{2}}$, это среднее число по-

лучаемых открытых текстов не превышает единицу. А для нашего примера это число $\frac{|M(d)|^2}{|I|^d} = \frac{2^{2d}}{2^{5d}} = \frac{1}{2^{3d}}$ намного меньше единицы. Данный факт обосновывает предположение о единственности полученной конкатенации $x(i)x(j)$.

Модель 3. Предположим, что ключи множества $K(M(d))$ выбраны случайно и равновероятно из множества $|I|^d$. Известно [9], что среднее число опробований ключей на расшифрование шифрованного текста длины d до попадания расшифрованного текста в множество $M(d)$ открытых текстов есть:

$$\frac{|I|^d + 1}{|K(M(d))| + 1}.$$

Ранее отмечалось, что число открытых текстов $|K(M(d))| = |M(d)|$ много меньше $\sqrt{|I|^d}$. В частности, в приведенном ранее примере $M(d) = 2^d$ и $|M(d)|^2 = 2^{2d} \ll \ll (\sqrt{|I|^d})^2 = 2^{5d}$.

Данный факт обосновывает предположение о единственности конкатенации $x(i)x(j)$.

Заключение

Границы применения атак 1, 2 определены фиксированным значением d . Их можно расширить, введя предварительный этап опробования каждого возможного значения параметра d . Подсчет трудоемкости и надежности таких расширенных атак не вызывает затруднений. Методы криптографического анализа (атаки) делятся на бесключевые методы и на методы с предварительным определением ключа. Теорию К. Шеннона о недешифруемости совершенных шифров следует понимать как недешифруемость этих шифров при знании шифрованного текста для бесключевых атак на открытый текст. Представленные две атаки на шифр случайного гаммирования с расчетом параметров

их сложности говорят о том, что мнение о недешифруемости шифра случайного гаммирования ошибочно. Ряд публикаций использует теорию совершенных шифров

К. Шеннона, а ряд работ расширяют границы применимости этой теории. Результаты этих работ следует теперь понимать с учетом указанного вывода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Shannon C. E. Communication theory of secrecy systems // The Bell system technical journal. — 1949. — Vol. 28. — № 4. — P. 656–715.
2. Шеннон К. Работы по теории информации и кибернетики / К. Шеннон. — М.: Рипол Классик, 1963. — 830 с.
3. Katz J., Lindell Y. Introduction to modern cryptography. — London: CRC Press, 2008. — 553 p.
4. Schneier B. Applied Cryptography. Second Edition: Protocols, Algorithms, and Source Code in C by Wiley Computer Publishing. — John Wiley & Sons, 1996. — 666 p.
5. Алферов А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. — М.: Гелиос АРВ, 2003. — 480 с.
6. Бабаш А. В. Совершенные шифры и как к ним относиться / А. В. Бабаш, Е. К. Баранова // Методы и технические средства обеспечения безопасности информации: Материалы 27-й научно-технической конференции, Санкт-Петербург, Россия, 24–27 сентября 2018 года. — СПб.: Издательство Политехнического университета, 2018. — С. 77–81.
7. Babash A. V. et al. Theoretically unbreakable ciphers as they should be understood // Theoretical questions of computer science, computational mathematics, computer science and cognitive information technologies. — 2018. — Vol. 14. — № 3. — P. 573–577. — DOI: 0.25559/SITI-TO.14.201803.573–577
8. Бабаш А. В. Совершенные шифры. Один новый совершенный шифр / А. В. Бабаш, Е. К. Баранова // Методы и технические средства обеспечения безопасности информации: Материалы 27-й научно-технической конференции, Санкт-Петербург, Россия, 24–27 сентября 2018 года. — СПб.: Издательство Политехнического университета, 2018. — С. 77–81.
9. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. — М.: СОЛОН-ПРЕСС, 2007. — 512 с.
10. Бабаш А. В. Избранные вопросы криптоанализа шифра случайного гаммирования / А. В. Бабаш, Е. К. Баранова // Методы и технические средства обеспечения безопасности информации. Сборник материалов 28-й научно-технической конференции, Санкт-Петербург, Россия, 24–27 июня 2019 года. — СПб.: Издательство Политехнического университета, 2019. — № 28. — С. 76–77.
11. Friedman W. F. The Index of Coincidence and Its Applications in Cryptology. — Geneva, Illinois, USA: Riverbank Laboratories, 1922. — 95 p.
12. Kasiski F. W. Die Geheimschriften und die Dechiffrier-Kunst. — Berlin: Mittler & Sohn, 1863. — 95 p.
13. Васильева И. Н. Криптографические методы защиты информации / И. Н. Васильева. — М.: Юрайт, 2016. — 64 с.
14. Салий В. Н. Криптографические методы и средства защиты информации: учебное пособие / В. Н. Салий. — Саратов, 2017. — 45 с.
15. Цыганов А. В. Криптография и криптоанализ / А. В. Цыганов. — Спб.: Из-во СПбГУ, 2009. — 60 с.
16. <http://mindhalls.ru/gamma-code/> (программа 12.08.2019).
17. Banks M. J. A Search-Based Tool for the Automated Cryptanalysis of Classical Ciphers. — The University of York. Department of Computer Science, 2008. — 76 p.

**Правила представления
статьей в журнал
«Проблемы информационной безопасности.
Компьютерные системы»**

1. На каждую статью обязательно оформляются экспертное заключение и рецензия.
2. Название статьи – на русском и английском языках.
3. Краткая аннотация – на русском и английском языках после названия статьи.
4. УДК – сверху, перед фамилией автора.
5. Размещение текста статей – в одну колонку, шрифт Times New Roman, кегль 12.
6. Шрифт заголовка статьи – кегль 12, жирный.
7. Внутри статьи соблюдается нумерация разделов и подразделов.
8. Формулы набирают в текстовом файле, формульный редактор MathType, латинские буквы – курсивом, греческие – прямым.
9. Векторы в формулах – жирным шрифтом.
10. Подрисуночные подписи и заголовки таблиц – кегль 11, жирный.
11. Текст программы оформляется рамкой.
12. Список литературы оформляется по ГОСТ 7.1–2003 с выделением жирным шрифтом фамилий авторов.

*Главный редактор журнала
П. Д. Зегжда*

**ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОМПЬЮТЕРНЫЕ СИСТЕМЫ**

№ 3, 2020

Редактор *Мирошникова Е. П.*
Корректор *Мирошникова Е. П.*
Компьютерная верстка *Н. В. Стасеевой*
Дизайн обложки *Т. М. Ивановой*

Налоговая льгота — Общероссийский классификатор продукции
ОК 005-93, т. 2; 95 3004 — научная и производственная литература

Подписано в печать 03.12.2020. Формат 60×84/8.
Усл. печ. л. 16,5. Тираж 100. Заказ 3253.

Отпечатано в Издательско-полиграфическом центре
Политехнического университета.
195251, Санкт-Петербург, Политехническая ул., 29.
Тел.: (812) 552-77-17; 550-40-14.