Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2021-25-4-52-69

Разработка генератора псевдослучайных чисел на основе кубических радикалов

М.О. Таныгин [1], Л.С. Крыжевич [2] ✉, П.С. Зыков [2]

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305040, Российская Федерация

[2] Курский государственный университет,
ул. Радищева, д. 33, г. Курск 305000, Российская Федерация

✉ e-mail: Leonid@programist.ru

Резюме

Цель исследования. *Главной опасностью при передаче конфиденциальных данных является их утечка. Организациями применяются различные меры защиты конфиденциальных данных, в которые входят и принятие нормативных документов для регламентации действий сотрудников, и применение технических средств защиты помещений, и установка программных продуктов. Ассиметричные методы обладают высоким уровнем стойкости, но достаточно вычислительно трудоемки. А различные подходы с использованием симметричных криптосистем сталкиваются с проблемами генерации и передачи ключа абонентам. Так возникает противоречие, связанное с криптографическим преобразованием конфиденциальных данных с небольшой вычислительной стоимостью и высоким уровнем защиты. В связи с этим, цель данного исследования заключается в снижении рисков безопасности конфиденциальной информации в организации с помощью повышения эффективности защиты каналов связи от утечки информации криптографическими методами.*

Методы. *В предложенном методе предлагается при реализации ассиметричного алгоритма шифрования на блоки исходного сообщения накладывать цепочку ключей, полученных путем генерации псевдослучайной последовательности на базе кубических радикалов. Этот подход гарантирует отсутствие периодичности чисел в блоках и неограниченную длину псевдослучайной последовательности.*

Результаты. *Полученные в ходе имитационного моделирования результаты показали, что данные цепочки чисел имеют равномерный характер распределения, могут делиться на блоки произвольной длины и с математической точки зрения не имеют периодичности.*

Заключение. *В работе показано, что применение рекурсивного алгоритма к генерации ключей позволяет снизить объем вычислительных затрат на 20 %, не теряя в уровне стойкости при одинаковых ключах. Приводится сравнительная таблица, демонстрирующая меньшие вычислительные затраты при одинаковой длине ключа по сравнению с другими популярными алгоритмами.*

Ключевые слова: *ассиметричное шифрование; генератор псевдослучайных последовательностей; кубические радикалы; криптографическая стойкость; криптоанализ .*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Таныгин М.О., Крыжевич Л.С., Зыков П.С. Разработка генератора псевдослучайных чисел на основе кубических радикалов // Известия Юго-Западного государственного университета. 2021; 25(4): 52-69. https://doi.org/10.21869/2223-1560-2021-25-4-52-69.

Поступила в редакцию 06.10.2021 *Подписана в печать 02.11.2021* *Опубликована 20.12.2021*

Development of a Pseudorandom Number Generator Based on Cubic Radicals

Maxim O. Tanygin [1], Leonid S. Kryzhevich [2] ✉, Peter S. Zykov [2]

[1] Southwest State University
50 Let Oktyabrya str. 94, Kursk 305040, Russian Federation

[2] Kursk State University
33, Radishcheva str., Kursk 305000, Russian Federation

✉ e-mail: Leonid@programist.ru

Abstract

Purpose of research. *The main danger in the transmission of confidential data is their leakage. Organizations take various measures to protect confidential data, which includes the adoption of regulatory documents to control the actions of employees, and the use of technical means of protecting premises, and the installation of software products. Asymmetric methods have a high level of durability, but are quite computationally time-consuming. In addition, various approaches using symmetric cryptosystems face the problems of generating and transmitting the key to subscribers. Therefore, there is a contradiction associated with the cryptographic transformation of confidential data with a small computational cost and a high level of protection. In this regard, the purpose of this study is to reduce the security risks of confidential information in the organization by increasing the effectiveness of protecting communication channels from information leakage by cryptographic methods.*

Methods. *In the proposed method, when implementing an asymmetric encryption algorithm, it is suggested to impose a chain of keys on the blocks of the original message obtained by generating a pseudo-random sequence based on cubic radicals. This approach guarantees the absence of periodicity of numbers in blocks and an unlimited length of a pseudo-random sequence.*

Results. *The results obtained during the simulation showed that these chains of numbers have a uniform distribution, can be divided into blocks of arbitrary length and, from a mathematical point of view, have no periodicity.*

Conclusion. *The paper shows that the application of a recursive algorithm to key generation reduces the amount of computational costs by 20%, without losing the level of durability for identical keys. A comparative table is provided that demonstrates lower computational costs with the same key length as compared to other popular algorithms.*

Keywords: *asymmetric encryption; pseudorandom sequence generator; cubic radicals; cryptographic strength; cryptanalysis.*

Conflict of interest. *The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Tanygin M. O., Kryzhevich L. S., Zykov P. S. Development of a Pseudorandom Number Generator Based on Cubic Radicals. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2021; 25(4): 52-69 (In Russ.). https://doi.org/ 10.21869/2223-1560-2021-25-4-52-69.

Received 06.10.2021 *Accepted 02.11.2021* *Published 20.12.2021*

***

Введение

Каналы связи облегчают передачу информации между пользователями и устройствами по всему миру. Растущее внедрение систем мобильной связи размыло изоляцию коммуникационных и вычислительных устройств от унифицированных информационных и коммуникационных систем. Это быстрое развитие и объединение коммуникационных и вычислительных технологий также открыло множество векторов для атак, многочисленных угроз и уязвимостей.

Каналы связи, используемые компаниями, продолжают расширяться по мере совершенствования технологий. Они дают работникам возможность сотрудничать и общаться как никогда раньше. Это делает компании более продуктивными и эффективными. Важные и конфиденциальные корпоративные данные проходят через мессенджеры, социальные сети, мобильные устройства и электронную почту. Следовательно, для специалиста по безопасности важно понимать и применять подходящие меры безопасности для устранения современных угроз и уязвимостей в коммуникационных технологиях [1].

Защита конфиденциальной информации от утечки – залог информационного здоровья любой компании, от небольшого юридического офиса до гигантского транснационального холдинга. Функционирование компаний в любой сфере деятельности связано с электронным документооборотом [2]. Это значит, что обработке могут подлежать персональные данные и коммерческая тайна, а значит требуется достаточная защита информации во избежание утечек.

Цель данного исследования заключается в снижении рисков безопасности конфиденциальной информации в организации с помощью повышения эффективности защиты каналов связи от утечки информации криптографическими методами.

Объектом исследования является передача конфиденциальной информации в компании по разработке программного обеспечения.

Предмет исследования – защита конфиденциальных данных от несанкционированного доступа при ее пересылке заказчику.

Материалы и методы

Фундаментальной задачей компьютерной безопасности является контроль информационного потока, будь то защита конфиденциальной информации от утечки или защита доверенной информации от искажения (рис.1).

Фактически, почти все организации, работающие с конфиденциальной информацией, например финансовые учреждения, военные учреждения или биржевые брокеры, сталкиваются с огромной проблемой обнаружения утечки [3] инсайдерской информации (табл.1).

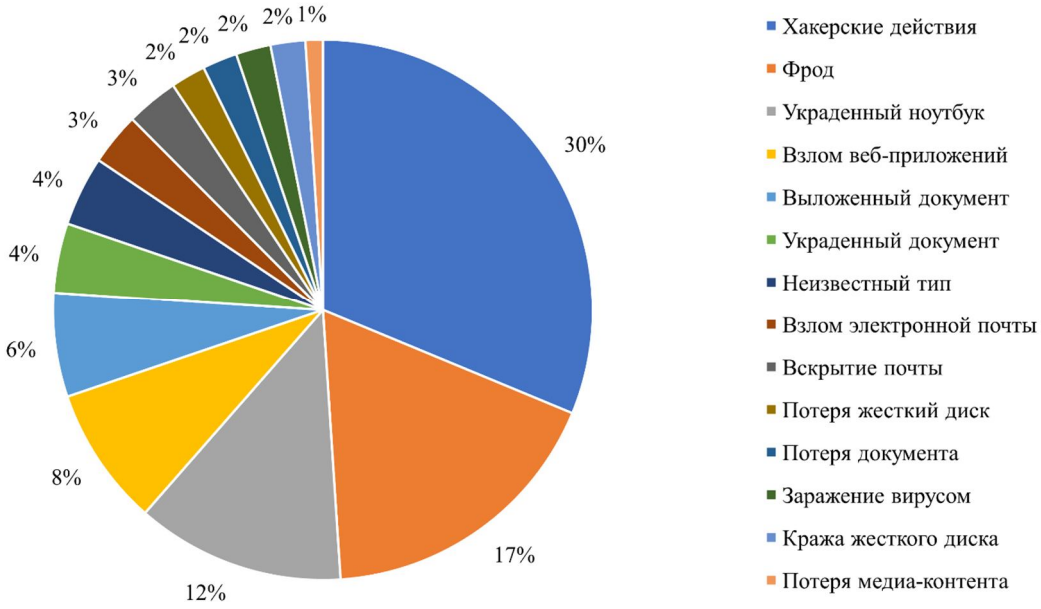

Рис. 1. Статистика по видам утечек

Fig. 1. Statistics on types of leaks

Таблица 1. Объекты, скомпрометированные в процессе атаки (в % от общего числа утечек/объема украденной информации)

Table 1. Objects compromised during the attack (in % of the total number of leaks/volume of stolen information)

Тип устройства / Device Type	Категория / Category	Все организации / All organizations	Крупные организации / Large organizations
POS-server	Серверы	50 / 1%	2 / <1%
POS terminal	Пользовательские устройства	35 / <1%	2 / <1%
Рабочая станция	Пользовательские устройства	18 / 34%	12 / 36%
Банкомат	Пользовательские устройства	8 / <1%	13 / <1%
Сервер Web-приложений	Серверы	6 / 80%	33 / 82%
Сервер СУБД	Серверы	6 / 96%	33 / 98%
Рядовые пользователи	Люди	3 / 1%	5 / <1%
Почтовый сервер	Серверы	3 / 2%	10 / 2%
Файловый сервер	Серверы	1 / <1%	5 / <1%
Ноутбуки	Люди	1 / <1%	5 / <1%
Сервер удаленного доступа	Серверы	1 / <1%	7 / <1%

Безопасность данных можно обеспечить с помощью их криптографических преобразований. Полагаясь на мнение специалиста по защите данных [4], можно говорить о том, что стремительное и динамичное развитие информационных технологий помимо всех имеющихся достоинств приводит также к появлению все большего количества угроз, уязвимостей и нарушителей, а значит есть необходимость усовершенствования и усиления систем обеспечения безопасности для защиты конфиденциальных сведений, коммерческой тайны от утечки.

Криптографические методы защиты данных

Для полной и адекватной защиты данных от несанкционированного доступа, необходимо применить как организационные меры, подразумевающие грамотную организацию режима допуска, методов, средств и мероприятий, снижающих уязвимость информации, так и технические меры. Но помимо применения организационных мер защиты ресурсов компании следует использовать технические, физические и программные средства [5].

Проверенный временем и опытом многих компаний способ защиты данных от несанкционированного доступа и утечки является использование криптографических преобразований, а если быть более точными – шифрования.

Повсеместное использование криптосистем привело к необходимости повышения стойкости используемых шифров. Впервые данный вопрос был проанализирован К. Шенноном в публикации 1949 года. В этой работе ученый сформулировал термин «совершенно стойкий шифр». Используя статистический подход, а именно вероятностную модель шифра, Шеннон доказал возможность существования стойких криптосистем на примере шифра Вернама («одноразовый блокнот») [6], показав, что количество информации можно измерять с помощью меры неопределенности случайной величины X – энтропии *H(X)*:

$$H(X) = \sum_{a:p(x)>0} p_x(a) \log_2 p_x(a),$$

где $p_x(a) = P[X = a]$, означает вероятность того, примет ли X значение a.

Согласно теории Шеннона, описанной в публикации «Математическая теория связи», в симметричных криптосистемах должны выполнять определенные принципы:

– рассеивание (diffusion): один знак открытого текста и один знак ключа должны влиять на более, чем один символ шифротекста;

– усложнение (confusion): криптографическое преобразование должно усложнять взаимосвязи между символами для затруднения восстановления исходных связей.

Также, во избежание атаки типа «противник посередине» (MITM), необходимо учесть условия для передачи ключей шифрования:

– равновероятные ключи, выбираемые из ключевого пространства случайным образом;

– противник, зная алгоритмы шифрования/расшифрования, не сможет взломать шифротекст без конкретного значения секретного ключа (условие Керкхоффса) [7].

Требования к современным криптосистемам расширяют и дополняют теорему Шеннона и имеют следующий вид:

– условие Керкхоффса: криптостойкость шифра не зависит от известности алгоритмов шифрования/расшифрования;

– сообщение можно расшифровать только при знании ключа;

– криптостойкость шифра не зависит от количества исходных данных и соответствующих им шифротекстов;

– дешифрование путем перебора (Brute force) должно требовать количества операций, имеющих нижнюю оценку, вычислительных мощностей, превосходящих возможности современных ЭВМ, или использования дорогостоящих систем;

– любое изменение ключа или исходных данных должно приводить к изменению шифротекста;

– неизменность структуры алгоритма шифрования/расшифрования;

– длина шифротекста должна совпадать с длиной исходного текста;

– если в процессе шифрования используется последовательно несколько ключей, зависимость между ними не должна легко определяться;

– все ключи из ключевого множества должны обеспечивать одинаковую надежную защиту данных.

Очевидно, что нельзя обеспечить стопроцентную безопасность или свести все риски к абсолютному нулю, особенно при использовании компьютерных вычислительных средств и Интернета. Однако необходимо пытаться свести все риски к минимуму, сохранив баланс между безопасностью, удобством использования технологий и ценой на обеспечение сохранности данных [8]. Исходя из всего вышеперечисленного можно прийти к выводу о том, что ассиметричное шифрование позволяет свободно обмениваться данными, что означает минимизацию трат на обеспечения выделенного канала связи [9], а также сохранение всех преимуществ (например, комфорт при использовании) среды, в которой происходит диалог (мессенджер, почта и т. д.)

Ассиметричное шифрование

Самыми распространёнными и часто используемыми алгоритмами являются: RSA, ECC, протокол Диффи-Хеллмана, схема Эль-Гамаля. Также ассиметричное шифрование используется в таких протоколах, как SSH, SSL, TLS: это нужно для установления соединения, передачи ключей симметричного шифрования. Также, ассиметричные методы применяются для формирования электронной подписи, чтобы подтвердить авторство и целостность сообщения [10].

Исходя из всего вышесказанного, можно прийти к выводу о том, что асимметричное шифрование разрешает

основное ограничение симметричного способа – использование одного ключа [11]. Поэтому для обмена данными можно пользоваться любым каналам связи, не опасаясь MITM-атак. Однако не обошлось и без недостатков: ассиметричные преобразования производятся долго, они гораздо медленнее симметричных.

Алгоритмическая модель шифрования данных

Основываясь на выводах, для обеспечения безопасной передачи данных был выбран ассиметричный способ шифрования, а именно схема Эль-Гамаля, поскольку в отличие от RSA, этот алгоритм не имеет патента, а значит не требует взносов за лицензию. Суть этой криптосистемы основана на сложности вычисления дискретных логарифмов.

Генерация ключей в данном алгоритме осуществляется следующим образом:

– генерируется случайное большое простое число p, при этом сообщение m должно быть меньше p;

– выбирается число g из множества целых чисел, являющееся первообразным корнем p;

– выбирается случайное число k из множества целых чисел, удовлетворяющее условиям:

k взаимно простое с числом (p – 1),

$1 < k < p - 1$.

Для понимания того, как работает алгоритм, необходимо подробно разобрать математические понятия. Первообразный корень по модулю p – это такое число из множества целых чисел, при котором

$$g^{\varphi(p)} \equiv 1 \pmod{p},$$

где $\varphi(p)$ – это функция Эйлера;

$$g^{l} \neq 1 \pmod{p} \text{ при } 1 \leq l < \varphi(p).$$

Для того, чтобы проверить, является ли число g первообразной p, необходимо, чтобы были соблюдены следующие условия:

Числа g и p – взаимно простые;

$$g^{\varphi(m)/2} \neq 1 (\mathrm{mod}\, p)$$

$g^{l} \neq 1 \pmod{p}$ для всех $l = \frac{\varphi(p)}{m}$, где m – это простой делитель $\varphi(p)$.

Шифрование производится следующим образом:

– отправитель и получатель генерируют секретные ключ k и q соответственно;

– отправитель и получатель рассчитывают открытые ключи и обмениваются ими:

$r_1 = g^k \pmod{p}$ – открытый ключ отправителя,

$r_2 = g^q \pmod{p}$ – открытый ключ получателя;

– отправитель выполняет преобразование:

$c = m \cdot r_2^k \pmod{p}$, где m – исходное сообщение;

получатель выполняет обратное преобразование:

$$m' = c \cdot (r_1^q)^{-1} \pmod{p} = c \cdot r_1^{p-1-q} \pmod{p}.$$

Модернизация алгоритма Эль-Гамаля на разделяемых ключах

Для модернизации алгоритма было принято решение генерировать не одну пару ключей для всего текста, а множество псевдослучайных ключей для каждого блока текста (вплоть до отдельного символа для потокового шифрования), в этом случае длина ключа будет равна длине текста, что значительно повысит криптостойкость алгоритма [12].

Поскольку главной проблемой асимметричных способов шифрования является низкая скорость преобразований, то было принято решение вычислять операции возведения в степень по бинарному методу возведения в степень с остатком, которые выполняются в памяти компьютера значительно быстрее.

Таким образом, усовершенствованный алгоритм шифрования выглядит следующим образом:

Выбор p – большого числа из множества простых чисел;

Выбор g – первообразного корня p;

Генерация цепочки случайных чисел K, мощность множества определяется длиной текста.

Расчет множества открытых ключей *R1* по формуле

$$R1_i = g^{K_i} \pmod p$$

Получение от получателя множества открытых ключей *R2*, мощность которого определяется длиной текста.

Шифрование каждого блока по формуле

$$c_i = m_i \cdot R2_i^{K_i} \pmod p.$$

Передача получателю множества (C, R1).

Соответственно обратный алгоритм выглядит следующим образом:

Выбор p – большого числа из множества простых чисел;

Выбор g – первообразного корня p;

Генерация множества случайных чисел G, мощность множества определяется длиной текста.

Расчет множества открытых ключей R2 по формуле

$$R2_i = g^{G_i} \pmod p.$$

Получение от получателя множества открытых ключей *R1*, мощность которого определяется длиной текста.

Шифрование и расшифрование каждого блока по формуле

$$c_i = m_i \cdot R2_i^{K_i} \pmod p;$$

$$m_i' = c_i \cdot R_1^{p-1-G_i} \pmod p.$$

Для дополнительного повышения криптостойкости алгоритма, было решено использовать для генерации случайных чисел k и q не встроенные методы генерации случайных чисел, а использование бесконечной псевдослучайной последовательности [13]. То есть, созданная последовательность должна казаться постороннему наблюдателю совершенной случайной, но давать возможность получателю сгенерировать её заново по определённому алгоритму.

В итоге, необходимо создание бесконечных, непериодических, псевдослучайных последовательностей [14].

Ярким примером такой последовательности может служить дробная часть иррационального числа. Иррациональные числа обладают следующими нужными нам свойствами:

1) обладают дробной частью бесконечной длины;

2) в дробной части числа нельзя выделить период (в отличии от рациональных чисел);

3) могут быть получены с помощью математических операций (извлечение корня, вычисления синуса, косинуса, тангенса или других тригонометрических операций, вычисление логарифма) [15].

В данной работе взят за основу метод последовательного нахождения радикала. Встроенные функции в различных языках программирования дают до 7-8 знаков после запятой (в редких случаях она достигает 19 знаков). Для решения поставленной задачи необходимо сгенерировать длинную цепочку цифр по длине секретного сообщения (может достигать 100 тысяч или даже 10 млн. символов).

Рассмотрим метод для извлечения кубического корня из целого числа:

1. Разобьём число справа налево на разряды по три цифры. Если бы количество цифр в числе было нечётным, то при разбиении его на разряды к первой цифре надо приписать нули.

2. Извлекаем кубический корень из старшего разряда с недостатком.

3. Возводим старший разряд в куб и вычитаем из первого разряда.

4. Приписываем к разности следующий разряд и слева от полученного числа ставим черту.

5. Приписываем перед вертикальной чертой удвоенное значение выражения, стоящего после знака «=», оставляя место под цифру, которое обозначим точкой.

6. Теперь необходимо подобрать такое число, на которое нужно умножить предыдущее выражение, чтобы получить выражение, стоящее после черты. Эта цифра будет последующей в итоговом числе.

7. Вычитаем из числа, стоящего после черты, произведение, описанное в предыдущем пункте, и повторим алгоритм, начиная с 5 шага, пока число не закончится.

Блок-схема алгоритма вычисления последовательных цифр представлена на рис. 2, где

p– исходное число,

kol – необходимое количество знаков после запятой,

a – целая часть от арифметического корня из исходного числа,

b – утроенное значение текущего результата,

y – остаток,

x – искомая цифра в числе,

i – номер текущего знака после запятой.

Криптоанализ стойкости алгоритма

Как утверждалось Ф.В. Касиски [16], чтобы шифр был устойчив ко взломам, необходимо равномерное распределение символов в ключе, иначе он может быть подобран глубоким частотным анализом.

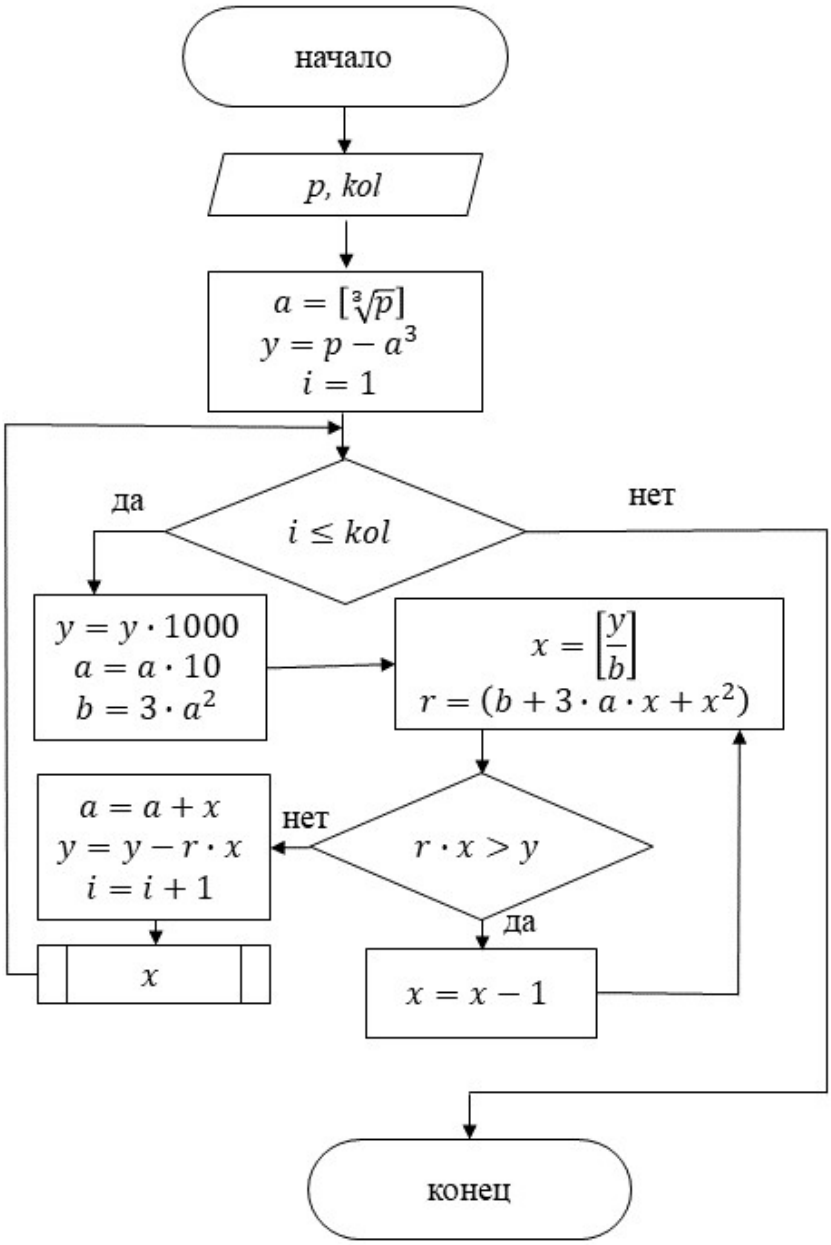

Рис. 2. Блок-схема генерации псевдослучайной последовательности на кубических радикалах

Fig. 2. Block diagram of pseudorandom sequence generation on cubic radicals

Однако в случае использования схемы Эль-Гамаля это избегается, поскольку секретные ключи k и q подбираются случайным образом (выбираются из псевдослучайной последовательности), а открытые ключи $R1$ и $R2$ вычисляются с помощью возведения в степень, а дискретное логарифмирование считается сложной задачей [17]. Рассмотрим гистограмму частот ключа R1 для текста в 100 000 символов (рис. 3).

Как видно, столбцы графика приходятся на степени двойки, что не дает вычислить символы по частоте их встречаемости.

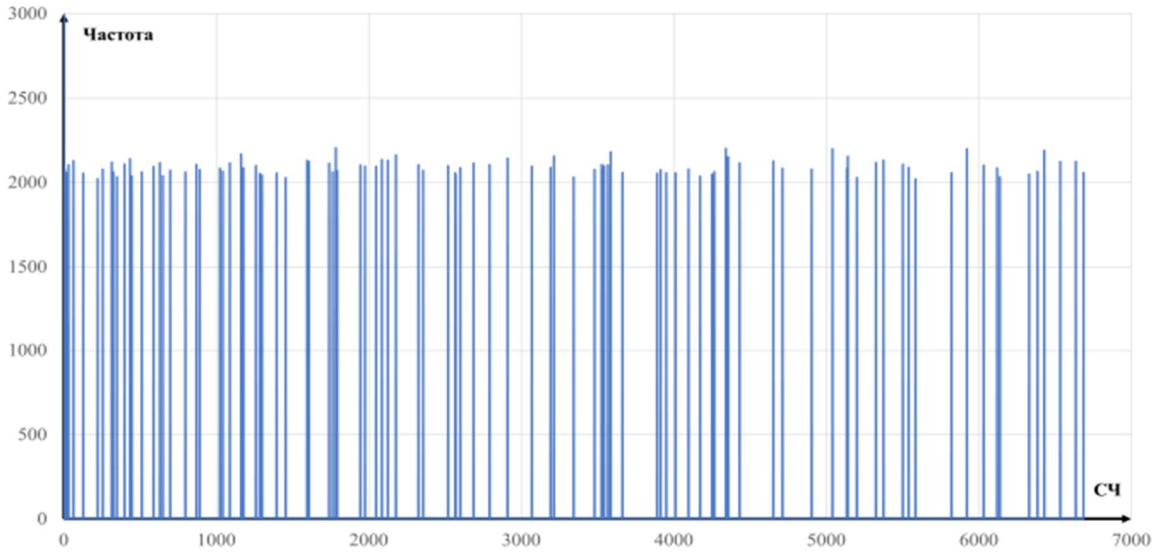

Рис. 3. Гистограмма частот

Fig. 3. Frequency histogram

Построим гистограмму частот для чисел k и q, чтобы убедиться, что все цифры после запятой распределены равномерно на примере вычисления корня из числа 17. Для сохранения криптостойкости проанализируем интервал от 100 до 200 знака после запятой. Получим следующие результаты (рис. 4)

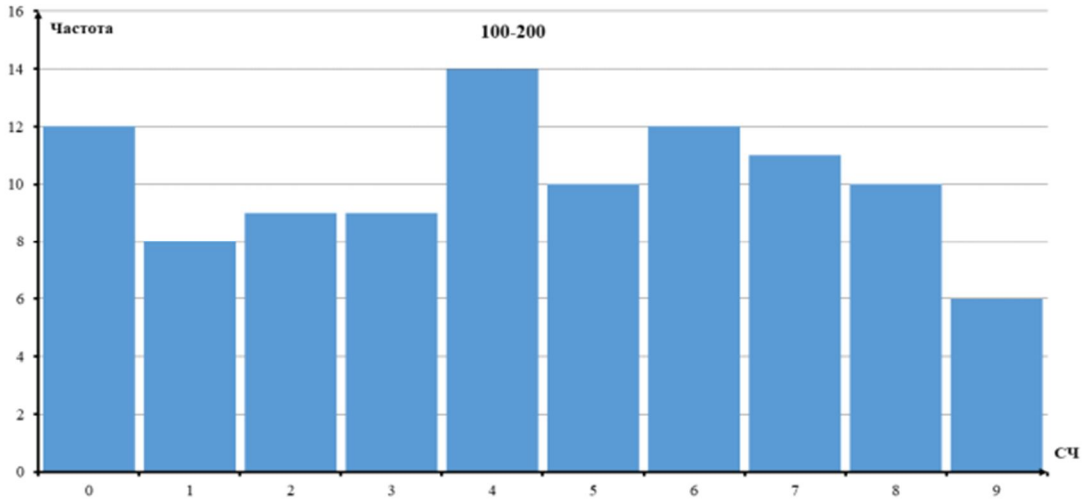

Рис. 4. Гистограмма распределения цифр в интервале от 100 до 200 знака

Fig. 4. Histogram of the distribution of digits in the range from 100 to 200 characters

Частота встречаемости каждой из цифр колеблется около 10, что подтверждает равномерное распределение цифр в радикале числа 3 [18].

Расширим интервал до 50000 знаков после запятой.

По диаграмме (рис. 5) можно обнаружить, что относительная частота встречаемости чисел от 0 до 99 число составляет около 1%, что также подтверждает гипотезу о равномерном распределении чисел после запятой в радикале просто-

го числа. При неизменной длине ключа криптостойкость алгоритма Эль-Гамаля равна $2{,}7 \cdot 10^{28}$ MIPS (англ. million instruction per second – миллион инструкций, осуществляемых процессором за секунду) для ключа 1300 бит [19].

Процесс шифрования текста представлен в табл. 2.

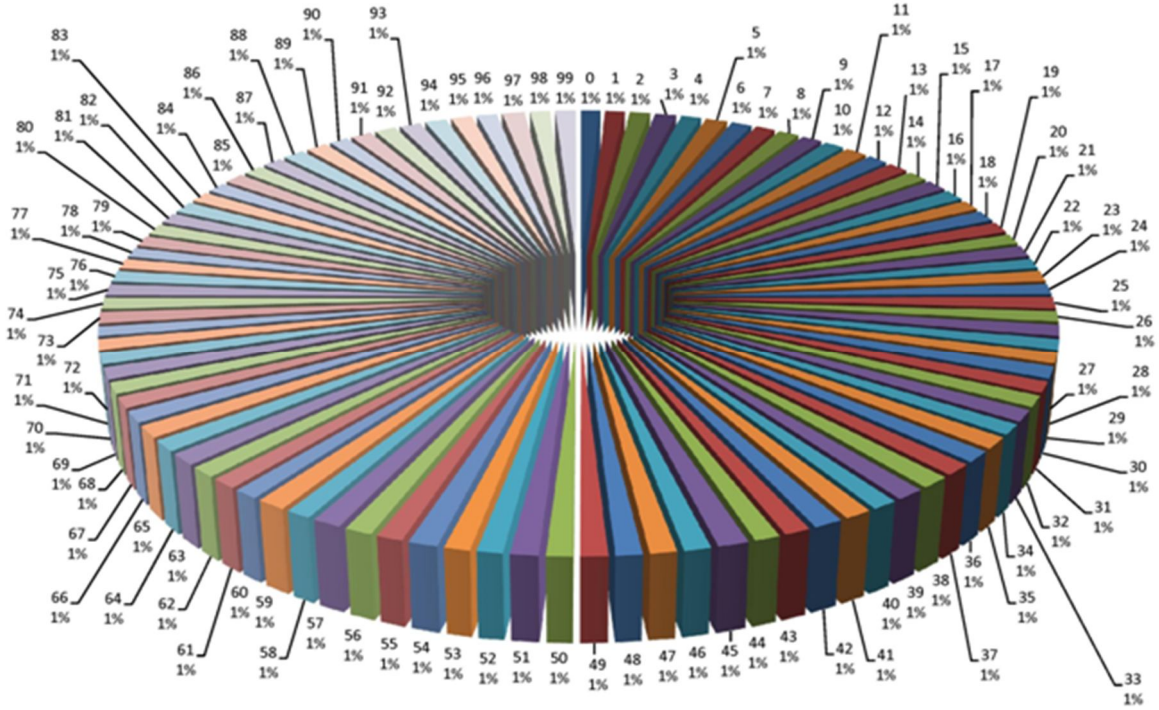

Рис. 5. Диаграмма распределения чисел от 0 до 99 в интервале от 1 до 50000 знака после запятой в радикале числа 17

Fig. 5. Diagram of the distribution of numbers from 0 to 99 in the range from 1 to 50000 decimal places in the radical of the number 17

Как видно из табл. 2, символ шифротекста (c) и открытого ключа ($R2_i$) для одной и той же буквы не совпадает, а значит их нельзя выявить частотным анализом или простым перебором [20].

Результаты и их обсуждение

Таким образом, выбранный алгоритм шифрования Эль-Гамаля был усовершенствован разделяемыми ключами для большей криптостойкости, а также была увеличена скорость работы алгоритма, за счет разделения более сложных операций (таких как возведение в степень) на простые составляющие.

Полученные в ходе имитационного моделирования результаты показали, что данные цепочки чисел имеют равномерный характер распределения, могут делиться на блоки произвольной длины и с математической точки зрения не имеют периодичности [21].

Выводы

Таким образом, было выявлено, что защита данных от утечки в любой компании – комплексный вопрос [22], имеющий большое значение для бизнес-процессов организации.

Таблица 2. Процесс шифрования текста

Table 2. Text encryption process

	m	k	r_1	q	r_2	c
В	1042	73	487	53	6443	3520
	32	66	1408	51	5206	745
л	1083	40	3047	73	487	3102
е	1077	38	6327	61	6521	4144
с	1089	20	2892	84	3304	2261
у	1091	12	5955	19	964	2438
	32	68	5935	38	6327	4142
р	1088	32	2088	98	2572	105
о	1086	20	2892	2	9	1175
д	1076	48	2688	52	2144	3347
и	1080	21	1939	93	371	2163
л	1083	91	3784	95	3339	393
а	1072	94	1113	89	1169	2487
с	1089	89	1169	57	2243	3608
ь	1100	75	4383	92	4615	6344
	32	90	3507	40	3047	3668
ё	1105	23	3977	23	3977	2199
л	1083	90	3507	52	2144	3461
о	1086	36	703	57	2243	1909
ч	1095	69	4331	49	1327	2073
к	1082	40	3047	97	3103	2415
а	1072	52	2144	68	5935	106

Таблица 3. Сравнение с аналогичными методами

Table 3. Comparison with similar methods

Критерии / Criteria	Метод гаммирования / XOR cipher technique	Метод RSA / RSA Method	Метод Эль-Гамаля / ElGamal technique	Метод на радикалах / Method based on radicals
Длина ключа	2048 бит	2048 бит	2048 бит	2048 бит
Криптостойкость	$3{,}2*10^{615}$ MIPS	$1{,}8*10^{308}$ MIPS	$3{,}2*10^{615}$ MIPS	$3{,}2*10^{615}$ MIPS
Мин. ширина блока	8 бит	256 бит	256 бит	16 бит
Время обработки при мин. ширине	256	256	2048	256
Макс. ширина блока	16 бит	2048 бит	2048 бит	1024 бит
Время обработки при макс.ширине	128	1408	15488	6400

В ходе выполнения работы была проведена деятельность по снижению рисков безопасности конфиденциальной информации в организации с помощью повышения эффективности защиты каналов связи от утечки информации криптографическими методами [23].

Для достижения этой цели были решены следующие научно-технические задачи:

– были определены виды каналов связи, выявлены и проклассифицированы потенциальные угрозы и уязвимости;

– были рассмотрены и изучены существующие технические меры и методы по защите конфиденциальной информации. Было выявлено, что актуальные способы защиты также имеют ограничения, а значит есть потребность в создании новых методов защиты данных;

– для защиты каналов связи от утечки информации была предложена усовершенствованная схема Эль-Гамаля на разделяемых ключах;

– применение рекурсивного алгоритма к генерации ключей позволяет снизить объем вычислительных затрат не теряя в уровне стойкости при одинаковых ключах.

Список литературы

1. Kalinin Maxim, Krundyshev Vasiliy, Zegzhda Peter. Cybersecurity risk assessment in smart city infrastructures // Machines. 2021. https://doi.org/10.3390/machines9040078.

2. Sukhanova N. Cryptographic information protection in distributed control systems – Science intensive technologies in mechanical engineering (2019). https://doi.org/ 10.37468/2307-1400-2021-2020-4-68-78. ISSN: 2307-1400.

3. Metelkov A. About cryptographic information protection measures in the implementation of information technology in the solution of management problems in the social and economic systems – National Security and Strategic Planning (2021). https://doi.org/ 10.37468/2307-1400-2021-2020-4-68-78. ISSN: 2307-1400.

4. Kaminskaya T. E., Kurbanova L. D. Retrospective and Prospects for the Development of Cryptocurrency – KnE Social Sciences (2018). https://doi.org/10.18502/kss.v3i2.1570.

5. Sukhanova Natalya V., Nakhushev Rakhim S. The Method of the Cryptographic Information Protection in IT -Systems // Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019 (2019). https://doi.org/10.1109/ ITQMIS.2019.8928348.

6. Sarwo B.B.P. Mulyana. Pengamanan file dokumen menggunakan kombinasi metode subtitusi dan Vigenere cipher – ILKOM Jurnal Ilmiah (2019). https://doi.org/ 10.33096/ ilkom.v11i3.477.222-230.

7. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis / H. Nelson, Carreras Guzman, Morten Wied, Igor Kozine, Mary Ann Lundteigen // Systems Engineering. 2020. https://doi.org/10.1002/sys.21509

8. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. Cryptographic Methods And Means Protection Transmitted Information in Telecommunication Systems // IFAC-PapersOnLine. 2018. https://doi.org/10.1016/j.ifacol.2018.11.187

9. Nesterenko A. Yu., Semenov A. M. On the practical implementation of Russian protocols for low-resource cryptographic modules // Journal of Computer Virology and Hacking Techniques. 2020.

10. Korolyov V., Ogurtsov M., Khodzinsky A. Multilevel Identification Friend or Foe of Objects and Analysis of the Applicability of Post-Quantum Cryptographic Algorithms for Information Security // Cybernetics and Computer Technologies. 2020. https://doi.org/10.34229/2707-451x.20.3.7. ISSN: 2707-4501.

11. Mohammad U.Q. Makki. A Review on Symmetric Key Encryption Techniques in Cryptography // International Journal of Computer Applications. 2016. https://doi.org/10.5120/ijca2016911203.

12. Rozlomii I. O. Researching structure and of cryptographic strength of the modification of gamma cipher // Electronics and Communications. 2016. https://doi.org/10.20535/2312-1807.2016.21.6.84112. ISSN: 1811-4512.

13. Beletsky A. Ya. Galois generalized matrices in stream ciphers // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika). 2020. https://doi.org/ 10.1615/TelecomRadEng.v79.i8.20. ISSN: 19436009.

14. Beletsky A. Generalized pseudorandom generators of the galois and fibonacci sequences // CEUR Workshop Proceedings. 2020.

15. Application of arithmetic coding methods in cryptographic information protection systems / D. Havrylov, O. Shaigas, O. Stetsenko, Y. Babenko, V. Yroshenko // CEUR Workshop Proceedings. 2021.

16. Tungatarova A.T., Borankulova G.S. Cryptographic method of information protection in computer training systems // Theoretical & Applied Science. 2017. https://doi.org/10.15863/tas.2017.05.49.21. ISSN: 23084944.

17. Rajan S., Mahendran D. S., John Peter S. Modified AES-256 algorithm with multiple-keys for secure data transmission and persistent storage // International Journal of Advanced Science and Technology. 2019. ISSN: 22076360.

18. Harold F. Tipton, Micki Krause Nozaki. Information security management handbook, sixth edition // Information Security Management Handbook, Sixth Edition. 2016. Vol. 6.

19. Moos T. Unrolled Cryptography on Silicon // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2020. https://doi.org/10.46586/tches.v2020.i4.416-442.

20. Xiang Yu, Jing Qiu, Xianfei Yang, Yue Cong, Lei Du. An graph-based adaptive method for fast detection of transformed data leakage in IOT via WSN // IEEE Access. 2019. https://doi.org/10.1109/ACCESS.2019.2942335

21. Sujoy Sinha Roy, Angshuman Karmakar, Ingrid Verbauwhede. Ring-LWE: Applications to cryptography and their efficient realization // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2016. https://doi.org/10.1007/978-3-319-49445-6_18, ISSN: 16113349.

22. Blagoev I. Neglected Cybersecurity Risks in the Public Internet Hosting Service Providers // Information & Security: An International Journal. 2020. https://doi.org/10.11610/isij.4704

23.. Cryptographic methods of information protection and VPN in IP networks / P.M. Movsarova, H.R. Vizirova, M.A. Bijsultanova, I.I. Gazieva, I.M. Daudov // Scientific development trends and education. 2019. https://doi.org/10.18411/lj-11-2019-38.

References

1. Kalinin M., Krundyshev V., Zegzhda P. Cybersecurity risk assessment in smart city infrastructures. *Machines*, 2021. https://doi.org/10.3390/machines9040078.

2. Sukhanova N. Cryptographic information protection in distributed control systems. *Science intensive technologies in mechanical engineering*, 2019. https://doi.org/10.37468/2307-1400-2021-2020-4-68-78. ISSN: 2307-1400.

3. Metelkov A.. About cryptographic information protection measures in the implementation of information technology in the solution of management problems in the social and economic systems. *National Security and Strategic Planning,* 2021. https://doi.org/10.37468/2307-1400-2021-2020-4-68-78. ISSN: 2307-1400.

4. Kaminskaya T. E., Kurbanova L. D.. Retrospective and Prospects for the Development of Cryptocurrency. *KnE Social Sciences,* 2018. https://doi.org/ 10.18502/kss.v3i2.1570.

5. Sukhanova N. V., Nakhushev R. S.. The Method of the Cryptographic Information Protection in IT -Systems. *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019*. https://doi.org/10.1109/ ITQMIS.2019.8928348.

6. Sarwo B.B.P. Mulyana. Pengamanan file dokumen menggunakan kombinasi metode subtitusi dan Vigenere cipher. *ILKOM Jurnal Ilmiah,* 2019. https://doi.org/ 10.33096/ilkom.v11i3.477.222-230.

7. Nelson H., Guzman C., Wied M., Kozine I., Lundteigen M. A.. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, 2020. https://doi.org/10.1002/sys.21509

8. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. Cryptographic Methods And Means Protection Transmitted Information in Telecommunication Systems. *IFAC-PapersOnLine*, 2018. https://doi.org/10.1016/j.ifacol.2018.11.187

9. Nesterenko A. Yu, Semenov A. M.. On the practical implementation of Russian protocols for low-resource cryptographic modules. *Journal of Computer Virology and Hacking Techniques,* 2020.

10. Korolyov V., Ogurtsov M., Khodzinsky A.. Multilevel Identification Friend or Foe of Objects and Analysis of the Applicability of Post-Quantum Cryptographic Algorithms for Information Security. *Cybernetics and Computer Technologies*, 2020. https://doi.org/ 10.34229/2707-451x.20.3.7. ISSN: 2707-4501.

11. Mohammad U.Q. Makki. A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*, 2016. https://doi.org/ 10.5120/ijca2016911203.

12. Rozlomii I. O. Researching structure and of cryptographic strength of the modification of gamma cipher. *Electronics and Communications*, 2016. https://doi.org/ 10.20535/ 2312-1807.2016.21.6.84112. ISSN: 1811-4512.

13. Beletsky A. Ya. Galois generalized matrices in stream ciphers. *Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika)*, 2020. https://doi.org/ 10.1615/TelecomRadEng.v79.i8.20. ISSN: 19436009.

14. Beletsky A. Generalized pseudorandom generators of the galois and fibonacci sequences. *CEUR Workshop Proceedings*, 2020.

15. Havrylov D., Shaigas O., Stetsenko O., Babenko Y., Yroshenko V.. Application of arithmetic coding methods in cryptographic information protection systems. *CEUR Workshop Proceedings*, 2021.

16. Tungatarova A.T., Borankulova G.S.. Cryptographic method of information protection in computer training systems. *Theoretical & Applied Science*, 2017. https://doi.org/ 10.15863/tas.2017.05.49.21. ISSN: 23084944.

17. Rajan S., Mahendran D. S., John Peter S. Modified AES-256 algorithm with multiple-keys for secure data transmission and persistent storage. *International Journal of Advanced Science and Technology*, 2019. ISSN: 22076360.

18. Tipton H. F., Micki Krause Nozaki. Information security management handbook, sixth edition. *Information Security Management Handbook*, *Sixth Edition*, 2016, vol. 6.

19. Moos T.. Unrolled Cryptography on Silicon. *IACR Transactions on Cryptographic Hardware and Embedded Systems,* 2020. https://doi.org/10.46586/tches.v2020.i4.416-442.

20. Xiang Yu, Jing Qiu, Xianfei Yang, Yue Cong, Lei Du. An graph-based adaptive method for fast detection of transformed data leakage in IOT via WSN. *IEEE Access*, 2019. https://doi.org/10.1109/ACCESS.2019.2942335

21. Sujoy Sinha Roy, Angshuman Karmakar, Ingrid Verbauwhede. Ring-LWE: Applications to cryptography and their efficient realization. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016. https://doi.org/10.1007/978-3-319-49445-6_18, ISSN: 16113349.

22. Blagoev I. Neglected Cybersecurity Risks in the Public Internet Hosting Service Providers. *Information & Security*: An International Journal (2020). https://doi.org/10.11610/isij.4704

23. Movsarova P.M., Vizirova H.R., Bijsultanova M.A., Gazieva I.I., Daudov I.M. Cryptographic methods of information protection and VPN in IP networks. *Scientific development trends and education,* 2019. https://doi.org/10.18411/lj-11-2019-38.

Информация об авторах / Information about the Authors

Таныгин Максим Олегович, кандидат технических наук, доцент, заведующий кафедрой «Информационная безопасность», Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru

Maxim O. Tanygin, Cand. of Sci. (Engineering), Associate Professor Faculty of Fundamental and Applied Computer Science, Southwest State University, Kursk, Russian Federation, e-mail: tanygin@yandex.ru

Крыжевич Леонид Святославович, кандидат технических наук, и.о. заведующего кафедрой «Информационная безопасность», Курский государственный университет, г. Курск, Российская Федерация, e-mail: Leonid@programist.ru

Leonid S. Kryzhevich, Cand. of Sci. (Engineering), Head of Information Security Department, Southwest State University,Kursk, Russian Federation, e-mail: Leonid@programist.ru

Зыков Петр Сергеевич, кандидат физико-математических наук, доцент кафедры «Информационная безопасность», Курский государственный университет, г. Курск, Российская Федерация, e-mail: petya39b@gmail.com

Peter S. Zykov, Cand. of Sci. (Physics and Mathematics), Associate Professor of Information Security Department, Southwest State University, Kursk, Russian Federation, e-mail: petya39b@gmail.com