УДК 004.654 DOI: 10.26102/2310-6018/2021.34.3.024

Способ прямого синтаксического преобразования данных как средство минимизации объема данных о событиях и инцидентах информационной безопасности

И.Д. Королев, Е.С. Литвинов, Д.И. Маркин, Е.А. Рогозин
Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, Краснодар, Российская Федерация

Резюме. Актуальность исследования обусловлена необходимостью повышения скорости и качества информационного обмена в информационных инфраструктурах, защищаемых средствами центров информационной защиты (security operation centers) в период активного вредоносного воздействия на канал связи, использовании высоконагруженных или низкоскоростных (нестабильных) каналов связи. В связи с этим, данная статья направлена на выявление способа (или метода) компрессии передаваемых данных в режиме реального времени (или с минимальными задержками), работающего с минимальными требованиями к привлекаемым ресурсам и позволяющего добиться максимально-возможного уровня сжатия данных. Методом к исследованию данной проблемы является сравнение возможностей и характеристик различных способов и методов компрессии данных в задаваемых условиях. Такой подход позволяет комплексно рассмотреть достоинства и недостатки каждого из предлагаемых способов и методов, а также осуществить выбор и оценку наиболее подходящего из них. В статье представлено большое количество различных способов и методов компрессии данных, раскрыты основные достоинства выбранного способа компрессии данных прямой синтаксической заменой, выявлены его достоинства и недостатки, обоснована необходимость использования именно этого способа для компрессии передаваемых данных о выявленных событиях и инцидентах информационной безопасности. Материалы статьи представляют практическую ценность для специалистов и разработчиков, работающих в области информационной безопасности, а также теоретическую ценность для учетных, осуществляющих свои исследования как в области информационной безопасности, так и в области информационных технологий в целом.

Ключевые слова: база данных, кодирование, компрессия, система управления базой данных, события и инциденты информационной безопасности, каналы связи

Для цитирования: Королев И.Д., Литвинов Е.С., Маркин Д.И., Рогозин Е.А. Способ прямого синтаксического преобразования данных, как средство минимизации объема данных о событиях и инцидентах информационной безопасности. *Моделирование, оптимизация и информационные технологии.* 2021;9(3). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1002 DOI: 10.26102/2310-6018/2021.34.3.024

A method of direct syntactic transformation of data as a means of minimizing the amount of data on information security events and incidents

I. D. Korolev, E. S. Litvinov, D. I. Markin, E. A. Rogozin
Krasnodar Higher Military Order of Zhukov and the October Revolution Red Banner School named after Army General S. M. Shtemenko, Voronezh, Russian Federation

Abstract: The relevance of the study is due to the need to improve the speed and quality of information exchange in information infrastructures protected by means of information security centers (security operation centers) during the period of active malicious impact on the communication channel, the use of high-load or low-speed (unstable) communication channels. In this regard, this article is aimed at identifying a method (or method) for compressing transmitted data in real time (or with minimal delays), working with minimal requirements for the resources involved and allowing you to achieve the highest possible level of data compression. The method to study this problem is to compare the capabilities and characteristics of various methods and methods of data compression under specified conditions. This approach allows you to comprehensively consider the advantages and disadvantages of each of the proposed methods and methods, as well as to select and evaluate the most appropriate one. The article presents a large number of different methods and methods of data compression, reveals the main advantages of the chosen method of data compression by direct syntactic replacement, identifies its advantages and disadvantages, and justifies the need to use this method for compressing transmitted data about identified events and incidents of information security. The materials of the article are of practical value for specialists and developers working in the field of information security, as well as theoretical value for researchers conducting their research both in the field of information security and in the field of information technology in general.

Keywords: database, coding, compression, database management system, information security events and incidents, communication channels

For citation: Korolev I.D., Litvinov E.S., Markin D.I., Rogozin E.A. A method of direct syntactic transformation of data as a means of minimizing the amount of data on information security events and incidents. *Modeling, Optimization and Information Technology*. 2021;9(3). Available from: https://moitvivt.ru/ru/journal/pdf?id=1002 DOI: 10.26102/2310-6018/2021.34.3.024 (In Russ).

Введение

Мировые тенденции в области защиты информации развиваются с огромной скоростью, предлагая новые и эффективные способы и методы защиты информации. Так, например, набирают популярность и широко используются в настоящее время специальные подразделения – центры информационной безопасности, обеспечивающие централизованную защиту различных цифровых инфраструктур как локально, так и удаленно [1-5].

Центры информационной безопасности осуществляют централизованное управление распределенными объектами автоматизированных систем управления, что подразумевает использование телекоммуникационных сетей для передачи данных о выявленных событиях и инцидентах информационной безопасности, сигналов и инструкций управления персоналом и средствами защиты информации [6-9]. Для качественного обеспечения безопасной обработки информации силами центров информационной безопасности, управление средствами защиты информации и мониторинг состояния контролируемых средств вычислительной техники должны отвечать требованиям оперативности и устойчивости в любых условиях [10-13].

Стоит обратить внимание на то, что пропускная способность каналов связи между объектами автоматизированных систем управления и удаленным центром информационной безопасности зависит как от технологий передачи данных, используемых провайдером, предоставляющим услуги связи, так и от финансовых возможностей предприятия.

Наиболее явно эта проблема выявляется в следующих условиях:

- при использовании высоконагруженных или нестабильных каналов связи;

- в условиях активного сетевого воздействия на канал связи или коммутационное оборудование (например, распределенная атака типа отказ в обслуживании) [14].

Данные условия сильно затрудняют реагирование центров информационной безопасности на явно выраженные инциденты информационной безопасности контролируемой автоматизированной системы.

Решение данной проблемы состоит в уменьшении объема передаваемых данных таким образом, при котором возможно осуществление обмена данными о событиях и инцидентах информационной безопасности в вышеописанных условиях.

Для осуществления компрессии передаваемых данных предлагается:

1) провести анализ существующих способов и методов преобразования данных;
2) определить особенности функционирования различных автоматизированных систем и центров информационной защиты;
3) осуществить выбор наиболее подходящего способа или метода компрессии данных.

Материалы и методы

В настоящее время уже известно большое количество способов и методов для сжатия данных, достаточно подробно описанных в книге «Методы сжатия данных» [15].

При этом, все способы и методы сжатия данных ориентированы на широкое применение, достаточно хорошо изучены и позволяют решать задачи транспортировки данных о выявленных событиях и инцидентах информационной безопасности, так как в качестве входного потока принимают как текстовые данные, так и байт-последовательности, которые могут формировать и текстовый документ, и графический рисунок или видеофильм [16,17]. Однако программы, основанные на этих методах, в большинстве случаев являются средствами предварительного кодирования, поскольку полная компрессия входного потока осуществляется до отправки, а декомпрессия – после получения, а значит требует дополнительных временных и вычислительных ресурсов [18-22]. При этом стоит отметить, что отдельные из представленных способов могут обеспечить сжатие информации в поточном режиме (например, способ Лемпеля-Зива, или методы построения контекстных моделей), однако для этого необходимо заблаговременно иметь схему преобразования, которая строится на основании вероятностей распределения отдельных элементов входного потока, а для подсчета этих вероятностей необходимо провести анализ входного потока.

Кроме того, не все из представленных методов и способов предназначены для компрессии данных и являются транфсормирующими (т. е. изменяющими структуру данных) и выполняются на этапе предобработки входного потока с целью повышения уровня сжатия данных на слушающих этапах.

Процесс прямого и обратного преобразования данных и последовательность выполнения действий показана на Рисунке 1. Таким образом, для получения наибольшего эффекта сжатия данных необходимо проводить анализ и оценку каждой из комбинаций способов преобразования информации и способов сжатия информации в зависимости от входного потока.

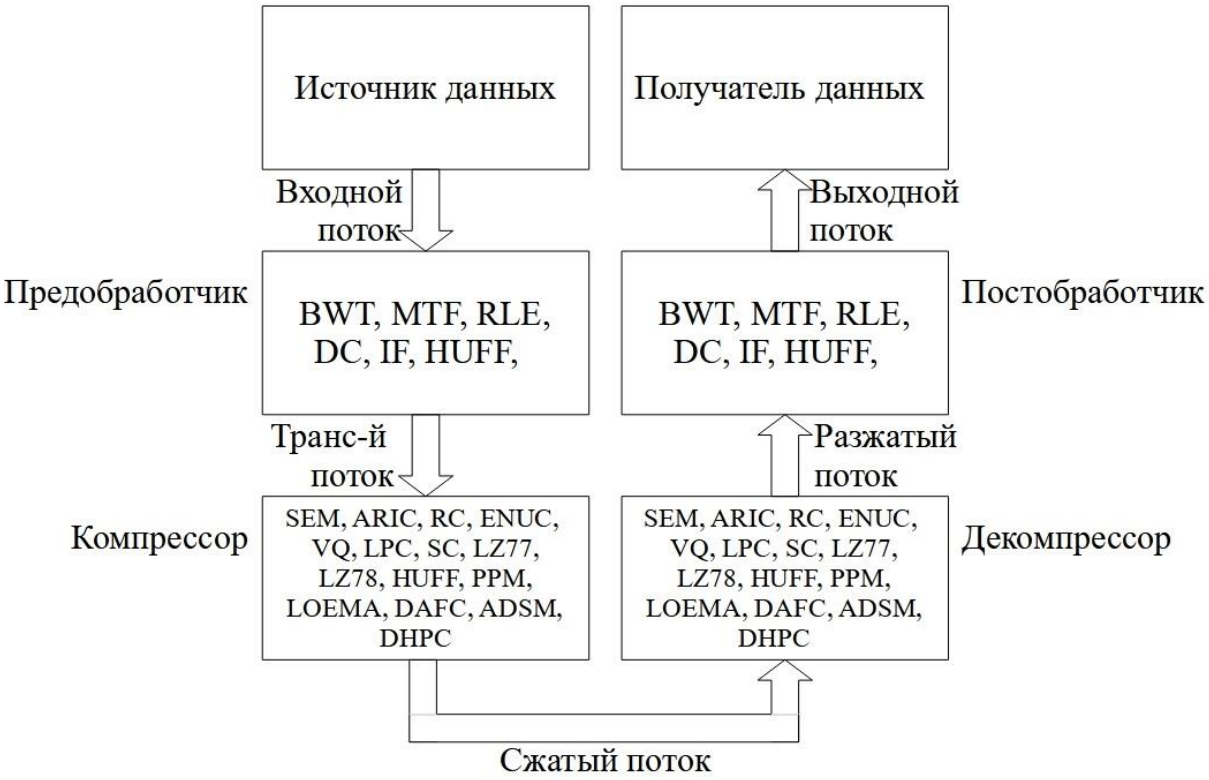


Рисунок 1 – Концептуальная модель процесса компрессии и декомпрессии данных
Figure 1 – Conceptual model of the data compression and decompression process

При этом, для такого большого разнообразия методик компрессии данных, в настоящее время порог среднего уровня компрессии равен значению энтропии входной последовательности (1) [15]:

$$H = -\sum_{k,i} P_k \cdot p_k(s_i) \log_2 p_k(s_i), \quad (1)$$

где:

s_i – элемент последовательности, подвергающийся процедуре кодирования;

$p(s_i)$ – вероятность появления элемента s_i в кодируемой последовательности;

P_k – вероятность принятия элементом s_i значения k.

Особое внимание необходимо уделить следующему фактору – все представленные ранее алгоритмы компрессии и преобразования предназначены для работы со входным потоком, представленным в формате байтовой строки или текста, без учета особенностей в форматировании этого текста.

В настоящее время данные о событиях и инцидентах информационной безопасности представляются в формате строки или кортежа данных, которые генерируются на источниках. При этом, данные о событиях и инцидентах информационной безопасности формируются по правилам реляционной алгебры (с различной степенью нормализации) и представляются в формате набора строк (кортежей), каждый элемент которого входит в состав домена. Размер таких доменов всегда будет конечным и задаваться либо производителями используемых программных и программно-аппаратных средств, либо персоналом на этапе ввода оборудования в эксплуатацию или его сопровождении.

Таким образом, средства, используемые центрами информационной защиты и выявляющие события и инциденты информационной безопасности заблаговременно уже

имеют некоторую шаблонную базу данных в формате информационного набора. Такое положение дел говорит о возможности заблаговременного накопления таких данных для формирования словаря. Использование такого словаря, который будет находиться на обоих сторонах информационного обмена способно значительно сократить объем передаваемых данных.

Для расчетов и построения модели информационного потока, содержащего данные о выявленных событиях и инцидентах информационной безопасности необходимо представить поток в следующем виде (2):

$$S = \{s_1, s_2, \ldots, s_n\}, \quad (2)$$

где:

S – строка, содержащая данные о выявленном событии и инциденте информационной безопасности, представляемая в виде мультимножества;

s_i – значение данных, принадлежащее домену $G(s)_i$.

Следует учесть тот факт, что значение вероятности выбора конкретного значения из домена G является величиной постоянной для каждого домена. Такой вывод сделан на основании того, что алфавит различных значений при регистрации событий и инцидентов информационной безопасности осуществляется в соответствии с кодировками, не учитывающими энтропию конкретного алфавита (3):

$$p(s_i) = \frac{1}{G(s_i)}. \quad (3)$$

Таким образом, уровень энтропии для одного элемента s_i будет равен (4):

$$H = \sum_{i=1}^{|S|} \log_2 G(s_i), \quad (4)$$

что позволяет осуществить расчет объема последовательности с помощью функции *Len* (5):

$$Len(\alpha) = \log_2 G(\alpha), \quad (5)$$

где:

α – последовательность, представленная в виде упорядоченного мультимножества;

$G(\alpha)$ – величина, определяющая размер домена, формируемого всеми допустимыми значениями мультимножества α. При этом величина α может быть представлена как единичным символом, так и набором таких символов (словом).

Исходя из того, что объем строки равен сумме объемов всех ее отдельных элементов (6):

$$Len(S) = \sum_{i=1}^{|S|} len(s_i), \quad (6)$$

следует (7):

$$Len(S) = \sum_{i=1}^{|S|} \left(\log_2 |G(s_i)|\right). \quad (7)$$

Основная идея прямого синтаксического кодирования заключается в замене символьных (словарных) величин, входящих в состав домена с большей мощностью, на символьные (словарные) величины, входящие в состав домена с меньшей мощностью, то есть (8):

$$G(s'_i) \le G(s_i) \Rightarrow Len(S') \le Len(S), \quad (8)$$

где:

S' – величина, позволяющая однозначно определить значение S;

s'_i – величина, позволяющая однозначно определить значение s'. При этом величина $|G(s'_i)|$ должна быть представлена с использованием минимально возможного набора символов (слов).

Необходимо также определить объем памяти, выделяемый для хранения таблицы преобразования (словаря синтаксической замены), который позволяет определить соответствия между элементами s и s'.

Исходя из того, что для одного значения s всегда будет иметься эквивалентная величина s', следует, что словарь будет занимать следующий объем (в битах) (9):

$$Len(M) = \sum_{i=1}^{|S|} \frac{\log_2\left(|G(s_i)| \cdot |G(s'_i)|\right)}{|\{S \mid s_i\}|}. \quad (9)$$

Таким образом, очевидно следующее:

1) увеличение вероятностей появления нового значения s влечет за собой и уменьшение объема словаря синтаксической замены;
2) объем словаря синтаксической замены имеет экспоненциальную зависимость от значений $G(s)$ и $G(s')$.

Результаты

Таким образом, при проведении компрессии данных о выявленных событиях и инцидентах информационной безопасности транспортировке будет подвергнут следующий объем информации (10):

$$Len(S') = \sum_{i=1}^{|S|} \log_2\left(|G(s'_i)|\right) + \sum_{i=1}^{|S|} \frac{\log_2\left(|G(s_i)| \cdot |G(s'_i)|\right)}{|\{S \mid s_i\}|}. \quad (10)$$

Особое внимание следует уделить тому, что наличие словаря синтаксической замены на обоих сторонах информационного обмена позволяет еще больше сократить объем передаваемых данных (11):

$$Len(S') = \sum_{i=1}^{|S|} \log_2\left(|G(s'_i)|\right). \quad (11)$$

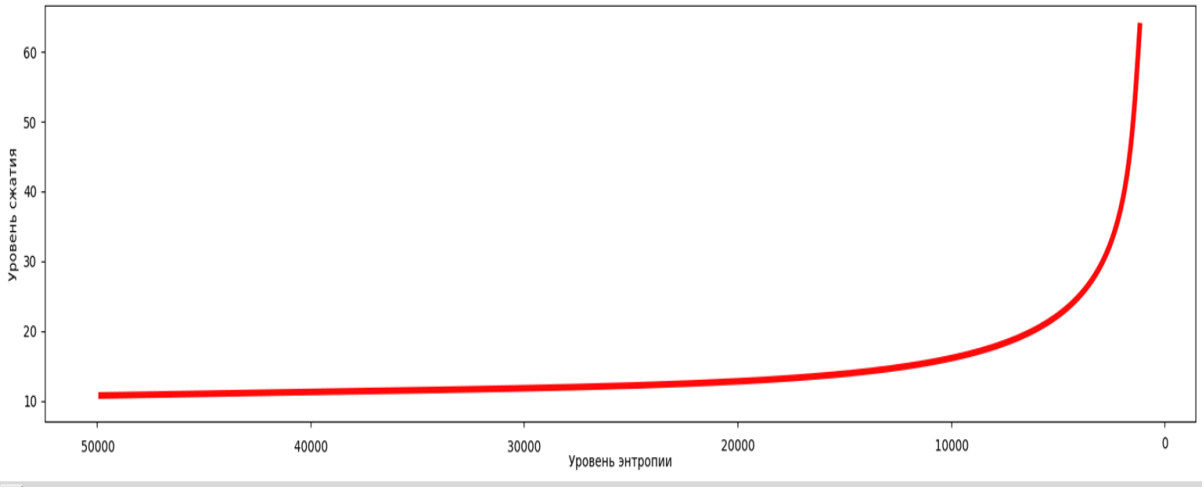
При этом уровень компрессии C при этом достигнет значения (12):

$$C = \sum_{i=1}^{|S|} \frac{\log_2 |G(s_i)|}{\log_2 |G(s'_i)|}. \quad (12)$$

При учете зависимости величины $G(s'_i)$ от уровня энтропии входной последовательности, получается (13):

$$C = \sum_{i=1}^{|S|} \frac{\log_2 |G(s_i)|}{H_s}. \quad (13)$$

Расчет уровня компрессии для различных уровней энтропии входной последовательности представлен на Рисунке 2 и наглядно показывает степень роста



уровня компрессии, в зависимости от значения уровня энтропии входной последовательности.

Рисунок 2 – Зависимость уровня сжатия от энтропии входного потока
Figure 2 – Dependence of the compression level on the entropy of the input stream

В качестве примера можно рассмотреть строку данных, формируемую средствами защиты информации, в соответствии со стандартом сетевого протокола Syslog (выбран исходя из его универсальной направленности, позволяющей использовать единую форму для формирования базы данных, в том числе и содержащих информацию о выявленных событиях и инцидентах информационной безопасности), а в качестве конкретного набора данных – список дат, в которые были выявлены различные события и инциденты. При этом, формат такой записи будет иметь вид: месяц (3 символа), день (2 символа), время (8 символов). При использовании таблицы кодировки ASCII (или родственных ей) или UTF-8, объем передаваемый данных для одной даты составляет 15 байт, а при использовании кодировки Unicode – 30 байт.

Несмотря на то, что набор символов, описывающих конкретное время и дату, может принимать практически любое значение (например, при формировании прогноза на ближайшее тысячелетие), а в отдельных случаях принимать отрицательные значения (при формировании отчета об археологических находках), размер домена дат о выявленных событиях и инцидентах информационной безопасности будет значительно меньше, и определяться периодом с даты подключение контролируемой системы к активам центра информационной защиты, до периода функционирования этой системы.

Проведем расчеты за период работы системы 5 лет. Размер домена для данных первого типа (месяц) равен 12, второго типа (день) – 31, третьего типа (время) – 86400. Используя формулу (4), можно рассчитать, что для компрессии первой группы данных необходимо 4 бита, второй группы – 5 бит, третьей группы – 17 бит.

Расчетные значения для представленных кодировок представлены в Таблице 1.

Таблица 1 – Расчет уровня компрессии для различных объемов выгрузки
Table 1 – Calculation of the compression level for different volumes of unloading

	Кодировка ASCII (UTF-8)	Кодировка ASCII (Unicode)
Объем 1 строки	120 бит	240 бит
Max объем за один год	0.4277 Гиб	0.8554 Гиб
Max объем за 5 лет	2.1386 Гиб	4.2772 Гиб
Max объем за один год (словарь сформирован заблаговременно)	0.4633 Гиб	0.4633 Гиб
Объем словаря	0.5203 Гиб	0.9481 Гиб
Max объем за один год (словарь не сформирован заблаговременно)	0.9837 Гиб	1.4114 Гиб
уровень компрессии без словаря	4.6153	9.2307
уровень компрессии со словарем	2.1739	3.0303

Заключение

Представленные расчеты наглядно показывают возможность осуществления кодирования данных о выявленных событиях и инцидентах информационной безопасности с получением максимально возможного уровня компрессии. Такой эффект достигается в связи с возможностью подготовки словаря синтаксической замены.

При этом, использование однородных средств защиты информации, средств мониторинга состояния сетевого оборудования, программных средств диагностирования, средств антивирусной защиты, контроля доступа и других программных и программно-аппаратных средств, генерирующих данные о выявленных событиях и инцидентах информационной безопасности, позволяет обеспечить формирование словаря прямой синтаксической замены на этапах ввода в эксплуатацию автоматизированных систем различного назначения или этапах модернизации таких систем.

Использование способа простой синтаксической замены позволяет значительно сократить объем передаваемых данных без утраты информативности, а значит и повысить скорость транспортировки таких данных, даже в условиях активного воздействия на канал связи со стороны нарушителя, погодных или других условий.

ЛИТЕРАТУРА

1. Weissman D., Jayasumana A. Integrating IoT monitoring for security operation center. *Global Internet Things Summit (GIoTS)*. 2020:1-6.
2. Kwon T., Song J.-S., Choi S., Lee Y. , Park J. VISNU: A novelvisualization methodology of security events optimized for a centralizedSOC. *13th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*. 2018:1–7.
3. Plachkinova M., Maurer C. Security Breach at Target. *Journal of Information Systems Education.* 2018;29:11-20.
4. Choong-Hee H., Soon-Tai P., Sang-Joonc L. The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection.* 2019;24:3-12.
5. David Janos F., HuuPhuoc Dai N. Security concerns towardssecurity operations centers inProc. *IEEE 12th Int. Symp. Appl.Comput. Intell. Informat. (SACI).* 2018;273–278.

6. Mihaela Oprea A., Li Z., Norris R., D Bowers K., MADE: Security Analytics for Enterprise Threat Detection. *Proceedings of the 34th Annual Computer Security Applications ConferenceDecember.* 2018:124–136.
7. Achmadi D., Suryanto Y., Ramli K. On developing information security management system (isms) framework for iso 27001-based data center. *2018 International Workshop on Big Data and Information Security (IWBIS).* 2018:149-157.
8. Petrenko S. Security Operations Center (SOC) Key Role. *Cyber security innovation for the digital economy.* 2018:150-162.
9. Miloslavskaya N. Developing a Network Security Intelligence Center. *Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society).* 2018:359-364.
10. Alali M., Almogren A., Mehedi Hassan M., Rassan I.A.L., BhuiyanMd.Z.A. *Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security.* 2018:323-339.
11. Ganesan R., Shah A. A Strategy for Effective Alert Analysis at a Cyber Security Operations Center. *A Strategy for Effective Alert Analysis at a Cyber Security Operations Center.* 2018:206-226.
12. Mutemwa M., Mtsweni J., Zimba L. Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC).* 2018:1-6.
13. Kuypers M.A., Maillart T., Pate-Cornell E. An empirical analysis of cyber security incidents at a large organization. *Department of Management Science and Engineering.* 2016:231-236.
14. Танэнбаум Э., Уэзэролл Д. *Компьютерные сети.* 2012:555-559.
15. Ватолин Д.С.. *Методы сжатия данных.* 2003:57-114.
16. K.R. Rao, P.X. Yip. *The Transform and Data Compression Handbook.* 2001:234-237.
17. Rissanen, J. A universal data compression system. *IEEE Trans. Inform. TheoryI.* 1983;29:656-664.
18. Iri N., Kosut O. Universal coding with point type classes. *51st Annual Conference on Information Sciences and Systems.* 2017:1-6.
19. Abdulmunem A.A., Mohammed D.J., Hassan A.K. Non-linear data structure for data coding for size compression. *1st International Conference of Pure and Engineering Sciences, ICPES 2020*. 2020.
20. Zhang Y., Lieven N.A.J., Nunez-Yanez J., Hutchinson P. Optimal compression of vibration data with lifting wavelet transform and context-based arithmetic coding. *25th EuropeanSignalProcessingConference, EUSIPCO 2017.* 2017;25:1996-2000.
21. He L., Dai B., Zhang D. Data compression for optical spectrum-encoding imaging system. *QiangjiguangYuLizishu.* 2018;30(9):99002.
22. Shurigin V.A., Makarov V.V., Vavrenyuk A.B., Starikovskiy A.V. Use of universal coding with binary thirds for information compression and its security. *International Journal of Soft Computing.* 2015;10(6):383-390.

REFERENCES

1. Weissman D., Jayasumana A. Integrating IoT monitoring for security operation center. *Global Internet Things Summit (GIoTS)*. 2020:1-6.
2. Kwon T., Song J.-S., Choi S., Lee Y. , Park J. VISNU: A novelvisualization methodology of security events optimized for a centralizedSOC. *13th Asia Joint Conf. Inf. Secur. (AsiaJCIS).* 2018:1–7.

3. Plachkinova M., Maurer C. Security Breach at Target. *Journal of Information Systems Education.* 2018;29:11-20.
4. Choong-Hee H., Soon-Tai P., Sang-Joonc L. The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection.* 2019;24:3-12.
5. David Janos F., HuuPhuoc Dai N. Security concerns towardssecurity operations centers inProc. *IEEE 12th Int. Symp. Appl.Comput. Intell. Informat. (SACI).* 2018;273–278.
6. Mihaela Oprea A., Li Z., Norris R., D Bowers K., MADE: Security Analytics for Enterprise Threat Detection. *Proceedings of the 34th Annual Computer Security Applications ConferenceDecember.* 2018:124–136.
7. Achmadi D., Suryanto Y., Ramli K. On developing information security management system (isms) framework for iso 27001-based data center. *2018 International Workshop on Big Data and Information Security (IWBIS).* 2018:149-157.
8. Petrenko S. Security Operations Center (SOC) Key Role. *Cyber security innovation for the digital economy.* 2018:150-162.
9. Miloslavskaya N. Developing a Network Security Intelligence Center. *Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society).* 2018:359-364.
10. Alali M., Almogren A., Mehedi Hassan M., Rassan I.A.L., BhuiyanMd.Z.A. *Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security.* 2018:323-339.
11. Ganesan R., Shah A. A Strategy for Effective Alert Analysis at a Cyber Security Operations Center. *A Strategy for Effective Alert Analysis at a Cyber Security Operations Center.* 2018:206-226.
12. Mutemwa M., Mtsweni J., Zimba L. Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC).* 2018:1-6.
13. Kuypers M.A., Maillart T., Pate-Cornell E. An empirical analysis of cyber security incidents at a large organization. *Department of Management Science and Engineering.* 2016:231-236.
14. Tanenbaum E., Weatherall D. *Computer networks.* 2012:555-559.
15. Vatolin D. S. *Data compression methods.* 2003:57-114.
16. K.R. Rao, P.X. Yip. *The Transform and Data Compression Handbook.* 2001:234-237.
17. Rissanen, J. A universal data compression system. *IEEE Trans. Inform. TheoryI.* 1983;29:656-664.
18. Iri N., Kosut O. Universal coding with point type classes. *51st Annual Conference on Information Sciences and Systems.* 2017:1-6.
19. Abdulmunem A.A., Mohammed D.J., Hassan A.K. Non-linear data structure for data coding for size compression. *1st International Conference of Pure and Engineering Sciences, ICPES 2020.* 2020.
20. Zhang Y., Lieven N.A.J., Nunez-Yanez J., Hutchinson P. Optimal compression of vibration data with lifting wavelet transform and context-based arithmetic coding. *25th EuropeanSignalProcessingConference, EUSIPCO 2017.* 2017;25:1996-2000.
21. He L., Dai B., Zhang D. Data compression for optical spectrum-encoding imaging system. *QiangjiguangYuLizishu.* 2018;30(9):99002.
22. Shurigin V.A., Makarov V.V., Vavrenyuk A.B., Starikovskiy A.V. Use of universal coding with binary thirds for information compression and its security. *International Journal of Soft Computing.* 2015;10(6):383-390.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Королёв Игорь Дмитриевич, доктор технических наук, профессор Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: pi_korolev@mail.ru
ORCID: 0000-0003-3102-4323

Korolev Igor Dmitrievich, doctor of technical sciences, professor of Krasnodar Higher Military School, Krasnodar, Russian Federation

Маркин Денис Игоревич, адъюнкт Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: denismark94@gmail.com
ORCID: 0000-0002-1616-7329

Markin Denis Igorevich, post-graduate student of Krasnodar Higher Military School, Krasnodar, Russian Federation

Литвинов Евгений Сергеевич, адъюнкт Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища им. С.М. Штеменко, Краснодар, Российская Федерация
e-mail: litvinoves@rambler.ru
ORCID: 0000-0003-1146-7370

Litvinov Evgeny Sergeevich, post-graduate student of Krasnodar Higher Military School, Krasnodar, Russian Federation

Рогозин Евгений Алексеевич, доктор технических наук, профессор, старший научный сотрудник Военного учебно-научного центра Военно-воздушных сил «Военно-воздушной академии имени профессора Н.Е. Жуковского и Ю.А. Гагарина», Воронеж, Российская Федерация
e-mail: evgenirogozin@yandex.ru
ORCID: 0000-0002-4455-7535

Rogozin Evgeny Alekseevich, Doctor of Technical Sciences, Professor, Senior Researcher of the Military Training and Research Center of the Air Force "Air Force Academy named after Professor N.E. Zhukovsky and Yu. A. Gagarin", Voronezh, Russian Federation

Статья поступила в редакцию 11.06.2021; одобрена после рецензирования 26.09.2021; принята к публикации 27.09.2021.

The article was submitted 11.06.2021; approved after reviewing 26.09.2021; accepted for publication 27.09.2021.