Современные инновации, системы и технологии // Modern Innovations, Systems and Technologies

2023; 3(2)
eISSN: 2782-2818
https://www.oajmist.com

УДК: 004.031.43
DOI: https://doi.org/10.47813/2782-2818-2023-3-2-0201-0212

EDN: QZOSNF

Глубокий интернет вещей

И. Н. Карцан[1,2], Е. А. Контылева[3]

[1]Морской гидрофизический институт РАН, г. Севастополь, Россия
[2]ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», г. Красноярск, Россия
[3]ФГАОУ ВО «Севастопольский государственный университет», г. Севастополь, Россия

Аннотация. Представлено исследование современных технологий и инструментов, используемых в глубоком интернете, а также оценка связанных с ними рисков. В связи с тем, что тот интернет, которым мы пользуемся ежедневно, называют «поверхностной сетью» (от англ. «surface web»), то для получения доступа к такому интернету не нужны специальные средства, достаточно работающего подключения. Все страницы «поверхностного» интернета легко найти с помощью любого поисковика с релевантным поиском, а действия пользователей в такой сети и данные о запросах и результаты поиска доступны интернет-провайдерам, поэтому данная работа представляет интерес для исследователей в области информационной безопасности, а также для тех, кто хочет более глубоко понимать технологии и риски, связанные с глубоким интернетом. В представленной работе проведена оценка глубокого интернета, проанализированы некоторые преступления с их последствиями и методы борьбы с ними, а также будущие возможности, принудительные методы и будущие маневры для уменьшения угрозы преступности.

Ключевые слова: глубокий интернет, технологии, инструменты, безопасность, риски, релевантность поиска.

Благодарности: Работа выполнена в рамках государственного задания по теме № FNNN-2021-0005.

Для цитирования: Карцан, И. Н., & Контылева, Е. А. (2022). Глубокий интернет вещей. Современные инновации, системы и технологии - Modern Innovations, Systems and Technologies, 3(2), 0201–0212. https://doi.org/10.47813/2782-2818-2023-3-2-0201-0212

The deep internet of things

Igor Kartsan[1,2], Elena Kontyleva[3]

[1]Marine Hydrophysical Institute, Russian Academy of Sciences, Sevastopol, Russia
[2]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia

[3]*Sevastopol State University, Sevastopol, Russia*

Abstract. A study of modern technologies and tools used in the deep Internet, as well as an assessment of the risks associated with them, is presented. Due to the fact that the Internet that we use every day is called the "surface web" to access such an Internet does not need special tools, a working connection is enough. All pages of the "surface" Internet can be easily found using any search engine with a relevant search, and the actions of users in such a network and data on requests and search results are available to Internet service providers, so this paper is of interest to researchers in the field of information security. The presented work assesses the deep internet, analyzes some crimes with their consequences and methods to combat them, as well as future opportunities, enforcement methods, as well as future maneuvers to reduce the threat of crime.

Keywords: deep web, technology, tools, security, risks, search relevance.

Acknowledgements: This study was supported by the Russian Federation State Task № FNNN-2021-0005.

For citation: Kartsan, I., & Kontyleva, E. (2022). The deep internet of things. Modern Innovations, Systems and Technologies, 3(2), 0201–0212. https://doi.org/10.47813/2782-2818-2023-3-2-0201-0212

ВВЕДЕНИЕ

Глубокий интернет является одним из самых сложных и не отслеживаемых средств, используемых киберпреступниками, террористами и шпионами для реализации своих незаконных целей. Киберпреступления, происходящие в глубоком интернете, похожи на преступления в реальном мире [1-8]. Однако огромные размеры, непредсказуемая экосистема и анонимность, обеспечиваемая сервисами глубокого интернета, являются основными препятствиями для отслеживания преступников. Чтобы найти потенциальные решения для борьбы с киберпреступностью, оценка угроз преступлений в глубоком интернете является важным шагом [9-15]. Глубокий интернет, также известный как Darknet, — это часть интернета, которая не доступна для обычных пользователей и требует специальных программ и настроек для доступа к ней. В последние годы глубокий интернет привлекает все большее внимание и становится объектом исследований в области информационной безопасности [7, 16-23]. Рассматривая современные технологии и инструменты, используемые в глубоком интернете, возможно оценить риски, связанные с ними.

МАТЕРИАЛЫ И МЕТОДЫ

Огромные размеры скрытой паутины требуют более эффективных подходов для минимизации потенциальных угроз со стороны глубокого интернета. Черный рынок и

транзакции, происходящие на просторах глубокого интернета, должны отслеживаться для обнаружения преступников с помощью передовых методов. Экосистема глубокого интернета очень непредсказуема, поскольку каждый день старые сайты исчезают, а новые появляются. При появлении новых сайтов, как правило, необходимы сильные цифровые доказательства для судебно-экспертных агентств [3, 10, 24-27].

Слои глубокого интернета можно разделить на три уровня: Первый уровень — это слой, который доступен через обычные браузеры и представляет собой веб-ресурсы, которые не индексируются поисковыми системами или имеют ограниченный доступ. Например, закрытые форумы, защищенные блоги, приватные почтовые сервисы и другие закрытые ресурсы. Второй уровень — это слой, который доступен через специальные программы и браузеры, такие как Tor. Этот уровень включает в себя защищенные ресурсы, которые требуют аутентификации пользователя и являются более безопасными, чем ресурсы первого уровня. К таким ресурсам относятся скрытые сайты, торговые площадки, финансовые сервисы, криптовалютные биржи и другие. Третий уровень — это самый глубокий слой глубокого интернета, который не доступен для общественного использования и используется для скрытой коммуникации и обмена информацией между различными организациями и группами. Этот уровень может быть доступен только через специальные сети, такие как Freenet или I2P [28-35].

Современные технологии и инструменты, используемые в глубоком интернете, играют важную роль в обеспечении анонимности и конфиденциальности пользователей. Среди таких технологий можно выделить Tor, I2P и Freenet.

Tor — это сеть анонимных серверов, созданная для обеспечения анонимности и конфиденциальности пользователей в интернете. Она позволяет пользователям обходить цензуру и ограничения, установленные в обычном интернете, и обеспечивает анонимный доступ к сайтам в сети Tor.

I2P — это анонимная сеть, которая предоставляет доступ к сайтам и сервисам, которые не доступны в обычном интернете. Она обеспечивает анонимность путем шифрования трафика и перенаправления его через различные узлы в сети I2P.

Freenet — это децентрализованная сеть, которая позволяет пользователям обмениваться информацией, обходя цензуру и ограничения, установленные в обычном интернете. Она использует шифрование для защиты данных, и все узлы в сети равноправны и не зависят от централизованной инфраструктуры.

Кроме того, в глубоком интернете используются криптографические протоколы [15-18, 36], такие как PGP и OTR, которые обеспечивают конфиденциальность и защиту данных. Протокол PGP, позволяет шифровать и расшифровывать сообщения, чтобы они были нечитаемыми для посторонних, а протокол OTR, обеспечивает конфиденциальность в переписке, предотвращая перехват сообщений и их подмену.

Технологии и инструменты, используемые в глубоком интернете, также включают в себя блокчейн-технологии, которые обеспечивают безопасность и надежность операций с криптовалютами, и технологии распределенных вычислений, которые позволяют использовать вычислительные мощности нескольких узлов в сети для выполнения сложных вычислительных задач.

РЕЗУЛЬТАТЫ

Глубокий интернет, как и любая другая технология, не лишен опасностей и рисков для пользователей. В этой части статьи мы определим и проанализируем наиболее значимые риски, связанные с использованием глубокого интернета.

Одним из главных рисков является возможность доступа к запрещенным материалам, таким как наркотики, оружие или детская порнография. В глубоком интернете существуют сайты, которые специализируются на распространении таких материалов, и доступ к ним может быть запрещен в большинстве стран мира. Также на таких сайтах может предлагаться нелегальная продукция или услуги, такие как оружие, контрабанда, убийства на заказ, что является серьезным правонарушением и может привести к уголовной ответственности.

Немаловажным риском является наличие киберпреступников, которые могут попытаться получить доступ к личным данным пользователей или использовать их компьютеры для майнинга криптовалют или атак на другие сайты. В глубоком интернете киберпреступники могут предлагать услуги по взлому аккаунтов, продаже украденной информации, кредитных карт и т.д. Такие преступные действия могут привести к утечке личной информации и финансовым потерям.

Еще одним риском является то, что многие сайты в глубоком интернете не имеют SSL-сертификатов, что делает передачу данных не защищенной и уязвимой для перехвата. Это может привести к утечкам личной информации, такой как логины и пароли. Кроме того, на таких сайтах может использоваться вредоносное программное обеспечение, которое может заражать компьютеры пользователей и украсть

конфиденциальную информацию, то есть могут не только нанести вред компьютеру, но и украсть личные данные пользователя.

Безопасность в глубоком интернете имеет решающее значение для защиты конфиденциальности, личной безопасности и сохранения данных. В глубоком интернете действует своя иерархия, законы и правила, которые отличаются от традиционных сетей. В связи с этим, безопасность в глубоком интернете может стать сложной задачей, требующей глубокого понимания технологий и умения обходить различные виды защиты.

Одним из основных средств обеспечения безопасности в глубоком интернете является использование специализированных программ, таких как браузеры Tor, I2P и Freenet, которые обеспечивают анонимность и шифрование данных. Однако, необходимо понимать, что такие программы не могут обеспечить абсолютную безопасность, так как существуют методы для их компрометации или атаки на уязвимости.

Для обеспечения безопасности в глубоком интернете следует использовать такие методы, как аутентификация, шифрование данных, использование анонимных платежных систем и использование виртуальных частных сетей (VPN). Также важно использовать антивирусное программное обеспечение и обновлять его регулярно.

Одним из наиболее серьезных рисков безопасности в глубоком интернете является возможность стать жертвой кибератак, которые могут привести к утечке личных данных, финансовым потерям или краже идентификационной информации. Поэтому, следует следить за тем, чтобы персональные данные были защищены, и они не должны разглашаться на площадках глубокого интернета, которые не вызывают уверенности в их безопасности.

ЗАКЛЮЧЕНИЕ

Глубокий интернет, несмотря на все риски, является важным ресурсом для исследователей, журналистов и людей, которые хотят обойти цензуру и получить доступ к информации, которая может быть запрещена или ограничена в их стране. Тем не менее, необходимо быть осторожным и принимать меры для обеспечения безопасности при использовании глубокого интернета. Кроме того, важно осознавать, что глубокий интернет не является абсолютно анонимным пространством, и следственные органы могут использовать различные методы, чтобы отслеживать и анализировать активности

пользователей. Поэтому необходимо использовать глубокий интернет только с законными целями и соблюдать законы и нормы этики. В целом, глубокий интернет представляет собой мощный ресурс, который может быть полезным для многих людей. Однако, использование этого ресурса также может иметь риски и опасности, которые необходимо учитывать. Поэтому важно принимать меры для обеспечения безопасности и защиты личных данных при использовании глубокого интернета.

Для выявления преступников в глубоком интернете необходимы дальнейшие исследования с использованием новых интеллектуальных способов, криптовалютных рынков и анализа дискуссионных форумов глубокого интернета.

СПИСОК ЛИТЕРАТУРЫ

[1] Терехов А. Deep Web: Мифы и реальность. Хакер. 2018; 2: 34-39.

[2] Голубев А.А., Ковалев А.В. Анонимность в сети Интернет: возможности и методы обеспечения. Информатика и ее применения. 2019; 13(2): 47-57.

[3] Морозов Е.С. Теневой интернет: правда и вымысел. Вестник Московского университета. Серия 10: Журналистика. 2019; 2: 83-97.

[4] Buxton J., Bingham T. The rise and challenge of dark net drug markets. Policy brief. 2015; 7: 1-24.

[5] Аверьянов В.С., Карцан И.Н. Методы оценки защищенности автоматизированных систем на базе квантовых технологий согласно CVSS V2.0/V3.1. Защита информации. Инсайд. 2023; 1(109): 18-23.

[6] Averyanov V.S., Kartsan I.N., Efremova S.V. Methods of automated detection of anomalies and nonlinear transitions by autonomous unmanned aerial vehicles. В сборнике: Journal of Physics: Conference Series. II International Scientific Conference on Metrological Support of Innovative Technologies (ICMSIT II-2021). 2021; 42001.

[7] Карцан И.Н., Жуков А.О. Механизм защиты промышленной сети. Информационные и телекоммуникационные технологии. 2021; 52: 19-26.

[8] Finklea K.M. Dark Web. in Proc. Congressional Res. Service. 2015; 1-16.

[9] Аверьянов В.С., Карцан И.Н. Безопасность ключевой последовательности по протоколу Чарльза Беннета. В сборнике: Российская наука, инновации, образование - РОСНИО-2022. 2022; 72-75.

[10] Карцан И.Н., Ярошенко М.В. Сжатие данных с помощью алгоритмов кодирования LZW и Хаффмана. В сборнике: Вопросы контроля хозяйственной деятельности и

финансового аудита, национальной безопасности, системного анализа и управления. материалы VII Всероссийской научно-практической конференции. 2022; 480-485.

[11] Ehney R., Shorter J.D. Deep Web, dark Web, invisible Web and the post isis world. Inf. Syst. 2016; 17(4): 36–41.

[12] Dolliver D.S., Kenney J.L. Characteristics of drug vendors on the Tor network: A cryptomarket comparison. Victims Offenders. 2016; 11(4): 600–620.

[13] Левин В.И., Барабаш А.Ю. Скрытые сети и службы сети Интернет. Материалы 13-й Международной научно-практической конференции «Наука и молодежь». 2018; 173-175.

[14] Карцан И.Н., Мордвинова А.Ю. Система управления информационными рисками. В сборнике: Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. Материалы VII Всероссийской научно-практической конференции. 2022; 141-146.

[15] Аксельрод В.А., Аверьянов В.С., Карцан И.Н. Протокол распределения квантовых ключей BB84 В сборнике: Российская наука, инновации, образование - РОСНИО-2022. Сборник научных статей по материалам Всероссийской научной конференции. 2022; 142-147.

[16] Açar K.V. Webcam child prostitution: An exploration of current and futuristic methods of detection. Int. J. Cyber Criminol. 2017; 11(1): 98–109.

[17] Chen H., Chung W., Qin J., Reid E., Sageman M., Weimann G. Uncovering the dark Web: A case study of jihad on the Web. J. Amer. Soc. Inf. Sci. Technol. 2008; 59(8) 1347–1359.

[18] Карцан И.Н., Гончаренко Ю.Ю. Влияние кибербезопасности на обработку информации в развивающихся новых технологиях. В сборнике: Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. Материалы VII Всероссийской научно-практической конференции. 2022; 471-479.

[19] Аверьянов В.С., Карцан И.Н. Об атаке расщепления в распределении криптографических ключей безопасности. Защита информации. Инсайд. 2022; 4(106): 20-23.

[20] Жуков А.О., Карцан И.Н., Аверьянов В.С. Информационная безопасность для проекта "Умный город". Информационные и телекоммуникационные технологии. 2021; 51: 39-45.

[21] Gai K., Qiu M., Tao L., Zhu Y. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Secur. Commun. Netw. 2016; 9(16): 3049-3058.

[22] Liu Q., Klucik R., Chen C., Grant G., Gallaher D., Lv Q., Shang L. Unsupervised detection of contextual anomaly in remotely sensed data. Remote Sens. Environ.,2017; 202: 75-87.

[23] Аверьянов В.С., Карцан И.Н. Запрещенный контент социокиберфизических систем: методы нейросетевой обработки информации. В сборнике: Информатика: проблемы, методы, технологии. Материалы XXII Международной научно-практической конференции им. Э.К. Алгазинова. 2022; 554-559.

[24] Аверьянов В.С., Карцан И.Н. Оценка защищенности киберфизических систем на основе общего графа атак. Южно-Сибирский научный вестник. 2022; 1(41): 30-35.

[25] Liu D., Wu Q., Han W., Zhou B. Sockpuppet gang detection on social media sites. Frontiers Comput. Sci. 2016; 10(1): 124-135.

[26] Maddox A., Barratt M.J., Allen M., Lenton S. Constructive activism in the dark Web: Cryptomarkets and illicit drugs in the digital demimonde. Inf., Commun. Soc., 2016; 19(1): 111-126.

[27] Аверьянов В.С., Каричев А.А., Карцан И.Н. Об атаках с явным исходом динамических переменных и криптостойкости ключей безопасности квантовых систем. Математические методы в технологиях и технике. 2022; 12(1): 29-34.

[28] Жуков А.О., Карцан И.Н., Аверьянов В.С. Кибербезопасность Арктической зоны. Информационные и телекоммуникационные технологии. 2021; 51: 9-13.

[29] Mishra P., Pilli E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in cloud environment: A survey. J. Netw. Comput. Appl. 2017; 77: 18-47.

[30] Chang D., Ghosh M., Sanadhya S.K., Singh M., White D.R. FbHash: A new similarity hashing scheme for digital forensics. Digit. Invest. 2019; 29: S113-S123.

[31] Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016; 55: 278-288.

[32] Жукова Е.С., Карцан И.Н. Обеспечение конфиденциальности информации в центре управления полетами. Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2009; 3(24): 93-97.

[33] Карцан Р.В., Жукова Е.С., Карцан И.Н. Универсальное программное обеспечение по типу "Каркас". Актуальные проблемы авиации и космонавтики. 2012; 1(8): 356-357.

[34] Карцан Р.В., Карцан И.Н. Дактилоскопия биометрический метод идентификации

на режимном предприятии. Актуальные проблемы авиации и космонавтики. 2013; 1(9): 405-406.

[35] Гурьянов К.В., Шатило Я.С. Организация противодействия распространению наркотиков через интернет. Антинаркотическая безопасность. 2016; 1(6): 101-108.

[36] Рогозин В.Ю., Вепрев С.Б. Криминализация интернета и web технологий. Расследование преступлений: проблемы и пути их решения. 2016; 3(13): 160-163.

REFERENCES

[1] Terekhov A. Deep Web: Myths and Reality. Hacker. 2018; 2: 34-39 (in Russian).

[2] Golubev A.A., Kovalev A.V. Anonymity in the Internet: opportunities and methods of ensuring. Informatics and its applications. 2019; 13(2): 47-57 (in Russian).

[3] Morozov E.S. Shadow Internet: truth and fiction. Vestnik (Herald) of Moscow University. Series 10: Journalism. 2019; 2: 83-97 (in Russian).

[4] Buxton J., Bingham T. The rise and challenge of dark net drug markets. Policy brief. 2015; 7: 1-24.

[5] Averyanov V.S., Kartsan I.N. Methods of security assessment of automated systems based on quantum technologies according to CVSS V2.0/V3.1. Inside. 2023; 1(109): 18-23 (in Russian).

[6] Averyanov V.S., Kartsan I.N., Efremova S.V. Methods of automated detection of anomalies and nonlinear transitions by autonomous unmanned aerial vehicles. In the collection: Journal of Physics: Conference Series. II International Scientific Conference on Metrological Support of Innovative Technologies (ICMSIT II-2021). 2021; 42001.

[7] Kartsan I.N., Zhukov A.O. Mechanism of industrial network protection. Information and telecommunication technologies. 2021; 52: 19-26 (in Russian).

[8] Finklea K.M. Dark Web. in Proc. Congressional Res. Service. 2015; 1-16.

[9] Averyanov V.S., Kartsan I.N. Key Sequence Safety by Charles Bennett Protocol. In the collection: Russian Science, Innovation, Education - ROSNIO-2022. 2022; 72-75 (in Russian).

[10] Kartsan I.N., Yaroshenko M.V. Data compression using LZW and Huffman coding algorithms. In the collection: Issues of control of economic activity and financial audit, national security, system analysis and management. materials of the VII All-Russian scientific-practical conference. 2022; 480-485 (in Russian).

[11] Ehney R., Shorter J.D. Deep Web, dark Web, invisible Web and the post isis world. Inf. Syst. 2016; 17(4): 36–41.

[12] Dolliver D.S., Kenney J.L. Characteristics of drug vendors on the Tor network: A cryptomarket comparison. Victims Offenders. 2016; 11(4): 600–620.

[13] Levin V.I., Barabash A.Yu. Hidden networks and services of the Internet. Proceedings of the 13th International Scientific-Practical Conference "Science and Youth". 2018; 173-175 (in Russian).

[14] Kartsan I.N., Mordvinova A.Yu. The system of information risk management. In the collection: Issues of control of economic activity and financial audit, national security, system analysis and management. Proceedings of the VII All-Russian Scientific and Practical Conference. 2022; 141-146 (in Russian).

[15] Axelrod V.A., Averyanov V.S., Kartsan I.N. Quantum key distribution protocol BB84 In the collection: Russian Science, Innovation, Education - ROSNIO-2022. Collection of Scientific Papers on Materials of All-Russian Scientific Conference. 2022; 142-147 (in Russian).

[16] Açar K.V. Webcam child prostitution: An exploration of current and futuristic methods of detection. Int. J. Cyber Criminol. 2017; 11(1): 98–109.

[17] Chen H., Chung W., Qin J., Reid E., Sageman M., Weimann G. Uncovering the dark Web: A case study of jihad on the Web. J. Amer. Soc. Inf. Sci. Technol. 2008; 59(8) 1347–1359.

[18] Kartsan I.N., Goncharenko Yu. In the collection: Issues of control of economic activity and financial audit, national security, system analysis and management. Proceedings of the VII All-Russian Scientific and Practical Conference. 2022; 471-479 (in Russian).

[19] Averyanov V.S., Kartsan I.N. About an attack of cleavage in distribution of cryptographic security keys. Information protection. Insider. 2022; 4(106): 20-23 (in Russian).

[20] Zhukov A.O., Kartsan I.N., Averyanov V.S. Information Security for the Smart City Project. Information and Telecommunication Technologies. 2021; 51: 39-45 (in Russian).

[21] Gai K., Qiu M., Tao L., Zhu Y. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Secur. Commun. Netw. 2016; 9(16): 3049-3058.

[22] Liu Q., Klucik R., Chen C., Grant G., Gallaher D., Lv Q., Shang L. Unsupervised detection of contextual anomaly in remotely sensed data. Remote Sens. Environ.,2017; 202: 75-87.

[23] Averyanov V.S., Kartsan I.N. Forbidden content of sociocyberphysical systems: methods of neural network information processing. In the collection: Informatics: problems, methods, technologies. Materials of XXII International Scientific and Practical Conference named after

E.K. Algazinov. 2022; 554-559 (in Russian).

[24] Averyanov V.S., Kartsan I.N. Assessment of cyberphysical systems security based on the general attack graph. South Siberian Scientific Bulletin. 2022; 1(41): 30-35 (in Russian).

[25] Liu D., Wu Q., Han W., Zhou B. Sockpuppet gang detection on social media sites. Frontiers Comput. Sci. 2016; 10(1): 124-135.

[26] Maddox A., Barratt M.J., Allen M., Lenton S. Constructive activism in the dark Web: Cryptomarkets and illicit drugs in the digital demimonde. Inf., Commun. Soc., 2016; 19(1): 111-126.

[27] Averyanov V.S., Karichev A.A., Kartsan I.N. About attacks with the explicit outcome of dynamic variables and cryptostability of security keys of quantum systems. Mathematical methods in technologies and techniques. 2022; 12(1): 29-34 (in Russian).

[28] Zhukov A.O., Kartsan I.N., Averyanov V.S. Cybersecurity of the Arctic Zone. Information and telecommunication technologies. 2021; 51: 9-13 (in Russian).

[29] Mishra P., Pilli E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in cloud environment: A survey. J. Netw. Comput. Appl. 2017; 77: 18-47.

[30] Chang D., Ghosh M., Sanadhya S.K., Singh M., White D.R. FbHash: A new similarity hashing scheme for digital forensics. Digit. Invest. 2019; 29: S113-S123.

[31] Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016; 55: 278-288.

[32] Zhukova E.S., Kartsan I.N. Ensuring confidentiality of information in the mission control center. Bulletin of Siberian State Aerospace University named after Academician M.F. Reshetnev. 2009; 3(24): 93-97 (in Russian).

[33] Kartsan R.V., Zhukova E.S., Kartsan I.N. Universal software by type "Karkas". Actual problems of aviation and cosmonautics. 2012; 1(8): 356-357 (in Russian).

[34] Kartsan R.V., Kartsan I.N. Dactyloscopy biometric method of identification at the regime enterprise. Actual problems of aviation and cosmonautics. 2013; 1(9): 405-406 (in Russian).

[35] Guryanov K.V., Shatilo Y.S. Organization of counteraction to the spread of drugs through the Internet. Anti-drug safety. 2016; 1(6): 101-108 (in Russian).

[36] Rogozin V.Y., Veprev S.B. Criminalization of the Internet and web technologies. Investigating crimes: problems and solutions. 2016; 3(13): 160-163 (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Карцан Игорь Николаевич, доктор технических наук, доцент, старший научный

Igor Kartsan, Dr. Sc., Associate Professor, Senior Researcher, Marine Hydrophysical

сотрудник Морского гидрофизического института РАН, Севастополь, Россия
e-mail: kartsan2003@mail.ru
ORCID: 0000-0003-1833-4036

Institute, Russian Academy of Sciences, Sevastopol, Russia

Контылева Елена Александровна, старший преподаватель кафедры Информационная безопасность, Севастополь, Россия
e-mail: eakontyleva@sevsu.ru

Elena Kontyleva, senior lecturer of the Department of Information Security, Sevastopol, Russia

Статья поступила в редакцию 28.04.2023; одобрена после рецензирования 19.05.2023; принята к публикации 22.05.2023.

The article was submitted 28.04.2023; approved after reviewing 19.05.2023; accepted for publication 22.05.2023.