Министерство науки и высшего образования РФ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет автоматики и вычислительной техники

Кафедра радиоэлектронных средств

Отчет по лабораторному практикуму №7

**Методика поиска НТИ на заданную тему**

дисциплина «Методология научных исследований»

|  |  |
| --- | --- |
| Выполнил: студент группы ИВТм-1301 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/Седов М.Д. / |
|  |  |
| Проверил: профессор кафедры РЭС | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Частиков А.В. / |

Киров 2021

**Цель**: овладеть методикой поиска НТИ на заданную тему. Научиться записывать библиографическое описание по ГОСТ.

**Задачи**:

1. Найти по два-три фундаментальных отечественных и зарубежных труда (монографий) по теме исследований.
2. Найти близкие по тематике исследований три-пять статей в отечественной периодике (за последние пять лет), например, по базе e-library. Записать их библиографическое описание по ГОСТ Р7.0.100-2018 (далее во всех пунктах).
3. Найти близкие по тематике три-пять статей в зарубежной периодике (за последние пять лет), например, в базах ieeexplore, Scopus и WoS.
4. Найти близкие по тематике пять диссертаций (не менее одной отечественной докторской диссертации и двух зарубежных диссертаций не более чем пяти-десятилетней давности).
5. Найти две-три депонированные рукописи за последние пять-десять лет по тематике исследований.
6. Найти близкие к теме исследований по три-пять публикаций (в тезисах или трудах) отечественных и зарубежных научно-технических конференций (симпозиумов) за последние пять лет.
7. Найти два-три отчета о НИР (ОКР), зарегистрированные в «Центре информационных технологий и систем органов исполнительной власти» (ЦИТиС) в период с 2011 по 2021 гг.
8. Найти по два патента пяти-семи ведущих стран по базам патентной информации. Глубина поиска – за последние пять-десять лет.
9. Составить сводный библиографический список литературы по ГОСТ Р7.0.100-2018.
10. Составить отчет в электронной форме. В отчете сделать обобщенные развернутые выводы. Отразить адекватность, репрезентативность, достаточность, доступность, актуальность, своевременность, точность, достоверность, устойчивость отобранной НТИ.

**1 Фундаментальные отечественные и зарубежные труды (монографии)**

**по теме исследований**

Тема научного исследования «Разработка программы моделирования передачи сообщений с асимметричным и симметричным шифрованием данных».

**1.1 Фундаментальные отечественные труды (монографии)**

1.1.1 Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. – 136 c. – Текст : непосредственный.

1.1.2 Коржик, В. И. Основы криптографии: монография / В. И. Коржик, В.А. Яковлев. – Санкт-Петербург: Интермедия, 2016 – 296 с. – Текст : непосредственный.

**1.2 Фундаментальные зарубежные труды (монографии)**

1.2.1 Goldreich, O. Foundations of Cryptography: A Primer : монография / O. Goldreich. – Almaty : Al-Farabi Kazakh National University Press, 2005. – 132 p. – Текст : непосредственный.

1.2.2 Lynn M.. Elliptic Curve Cryptography: монография / M. Lynn – Cambridge : Cambridge University Press, 2013. – 102 p. – Текст: непосредственный.

**2** **Статьи в отечественной периодике по теме исследований**

2.1 Смирнова, М. А. Асимметричное шифрование как способ проверки подлинности автора сообщения / М. А. Смирнова, И. А. Самойлова, Л. В. Устинова– Текст : непосредственный //Актуальные проблемы современности. – 2017. – № 2. – 5 с.

2.2 Умрзоков, С. Криптографические протоколы / С. Умрзоков – Текст : непосредственный // Мировая наука. – 2029. – № 6. – 5 с.

**3 Статьи в зарубежной периодике по теме исследований**

3.1 Xiaojuan Chen. Analysis of Cryptographic Protocol by Dynamic Epistemic Logic / Xiaojuan Chen, Huiwen Deng – Текст : непосредственный // IEEE. – 2019. – № 7. – 7 p.

3.2 Krishna Chaitanya Nunna. Secure Data Transfer Through Internet Using Cryptography and Image Steganography / Krishna Chaitanya Nunna – Текст : непосредственный // IEEE. – 2017. – №.12 – 7 p.

**4** **Отечественные и зарубежные диссертации по теме исследований**

Тема научного исследования «Разработка программы моделирования передачи сообщений с асимметричным и симметричным шифрованием данных».

**4.1 Отечественные диссертации по теме исследований**

4.1.1 Сизоненко, А. Б. Модели и алгоритмы синтеза логико-вычислительных подсистем защиты информации систем критического применения : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Сизоненко Александр Борисович; Воронежский институт МВД РФ. – Воронеж, 2016. – 310 с. – Текст: непосредственный.

4.1.2 Новиков, С. Н. Методология зашиты информации на основе технологий сетевого уровня мультисервисных сетей связи : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Новиков Сергей Николаевич; Томский государственный университет систем управления и радиоэлектроники. – Томск, 2016. – 235с. – Текст: непосредственный.

**4.2 Зарубежные диссертации по теме исследований**

4.2.1 Evmorfia-Iro Bartzia. A formalization of elliptic curves for cryptography. Doctoral dissertation / Evmorfia-Iro Bartzia; Université Paris Saclay. – 2017. – 127 p. – Текст : непосредственный.

4.2.2 Karpman, Pierre. Analysis of symmetric primitives. Doctoral dissertation / P. Karpman; Nanyang Technological University. – 2016. – 103 p. – Текст: непосредственный.

**5 Депонированные рукописи по тематике исследований**

5.1 Назаров, Н. И. Алгоритмы криптографии, использующие генераторы случайных или псевдослучайных чисел / Н. И. Назаров; Самарский государственный технический университет. – Самара, 2011. – 9 с. – Деп. в НТИЦ ГА от 31.08.2011 № 401-В2011. – Текст : непосредственный.

5.2 Бенсон, Я. Е. Моделирование динамических процессов / Я. Е. Бенсон, Е. Г. Зудов; Уральский государственный технический университет. – Екатеринбург, 2007. – 65 с. – Деп в ВИНИТИ РАН от 26.04.2007 № 1100-B2007 – Текст : непосредственный.

**6** **Публикации (в тезисах или трудах) отечественных и зарубежных**

**научно-технических конференций (симпозиумов)**

**6.1** **Публикации (в тезисах или трудах) отечественных**

**научно-технических конференций (симпозиумов)**

6.1.1 Мазунина, Е. С. Сквозное шифрование / Е. С. Мазунина. – Текст : непосредственный // Научное сообщество студентов. – 2016. – С. 48-50.

6.1.2 Казанцев, А.А. Криптография и криптоанализ / А. А. Казанцев. – Текст : непосредственный // Школьная секция: информационные технологии. – 2019. – C. 18.

**6.2 Публикации (в тезисах или трудах) зарубежных**

**научно-технических конференций (симпозиумов)**

6.2.1 Peng, Sheng-Lung. Proceedings of First International Conference on Mathematical Modeling and Computational Science / Sheng-Lung Peng, Hao, Rong-Xia, Pal, Souvik. – Текст : непосредственный // ICMMCS. – 2020.

6.2.2 Escalante, S. Automatic Recognition of Peruvian Car License Plates / S. Escalante, V. Murray. – Текст : непосредственный // Proceedings of the 2020 IEEE 27th International Conference on Electronics, Electrical Engineering and Computing, INTERCON 2020. – 2020.

**7 Зарегистрированные в ЦИТиС отчеты о НИР (ОКР)**

7.1 Математические алгоритмы криптографии / В.В. Меньших; руководитель НИОКТР к.т.н. Меньших В. В. // отчет о НИОКР, рег. номер: 07170612. – 2017. – 10с.

7.2 Основы информационной безопасности и защиты информации в ОВД / С.В. Крыгин, С.Н. Сухов, Т.Е. Чикина, А.О. Логинов; руководитель НИОКТР доктор физико-математических наук Крыгин С.В // отчет о НИОКР, рег. номер: 07170919; План научной деятельности на 2017 год Нижегородской академии МВД России; «Нижегородская академия МВД России». – 2017. – 129 с.

**8 Патенты ведущих стран по теме исследований**

**8.1 Россия**

8.1.1 Патент № 2544737 Российская Федерация, МПК RU 2520379 C2 (06.05.2021). Криптография на эллиптической кривой: № 2021616056/08 : заявл. 22.04.2021 : опубл. 06.05.2021 / Икар Тома, Корон Жан-Себастьен; заявитель Электро Грундлер (RU). – 17 с. : ил. – Текст : непосредственный.

8.1.2 Патент № 2617972 Российская Федерация, МПК RU 2016617549 A (20.06.2016. Криптографическое шифрование: № 2016108116 : заявл. 18.05.2016 : опубл. 07.07.2016 / Насыров Ринат Ришатович, Сулейманов Игорь Рашидович, Чуркин Андрей Игоревич.; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (RU). – 2 с. : ил. – Текст : непосредственный.

**8.2** **США**

8.2.1 United States Patent №: US 2017/0161614 A1, IPC G06N 5/02 (2006.01), G06F 7/50 (2006.01). Systems and methods for predicting emergency situations: Appl. No.: 15/371,117 : 6.12.2016 : Publication: 8.06.2017 / Anil Mehta, Michael John Martin, Nicholas Edward Horelik ; Assignee: Rapidsos Inc. (US). – 46 p. – Текст : непосредственный.

8.2.2 United States Patent №: US 2021/0186329 A1, IPC A61B 5/00 ( 2006.01 ), A61B 8/00 ( 2006.01 ), H04M 3/51 ( 2006.01 ), GO8B 21/04 ( 2006.01 ), G16H 50/20 ( 2006.01 ), G16H 15/00 ( 2006.01 ), G16Z 99/00 ( 2006.01 ), A61B 7700 ( 2006.01 ), A61B 5/318 ( 2006.01 ), A61B ( 2006.01 ), 5/369 ( 2006.01 ), A61B 5/389 ( 2006.01 ), A61B 5/01 ( 2006.01 ), A61B 5/0205 ( 2006.01 ). Mesh network personal emergency response appliance: Appl. No.: 17/177,282 : 17.02.2021: Publication: 24.06.2021 / Bao Tran(US); Assignee: KONINKLIJKE PHILIPS. – 77 p. – Текст : непосредственный.

**8.3 European Patent Office (EPO)**

8.3.1 European patent №: EP 2494525B1, IPC G06T 15/00 (2011.01), G03B 35/16 (2006.01), G06T 15/04 (2011.01). A method for automatic material classification and texture simulation for 3d models: Appl. No.: 14754127.0: 25.02.2014: Publication: 10.06.2020 / Peyman Moghadam; Assignee: Commonwealth Scientific and Industrial Research Organization CSIRO. – 30 p. – Текст : непосредственный.

8.3.2 European patent №: EP 2959459B1, IPC G06T 15/04 (2011.01) G06T 17/05 (2011.01). 3d-abbildungsverfahren und -system: Appl. No.: 10828764.0: 18.10.2010: Publication: 05.02.2020 / Stephen Schultz; Assignee: Pictometry International Corp. – 22 p. – Текст : непосредственный.

**8.4 Япония**

8.4.1 Japanese patent №: JP 5933632 B2, IPC G06F 3/0481 (2013.01), G05B 23/02 (2006.01). Graphic elements with multiple visualizations in a process environment: Appl. No.: 512132022: 13.05.2013: Publication: 15.06.2016 / Kyoomi Yamazawa, Kikuo Matsuzawa; Assignee: Seiko Instr & Electronics Ltd. – 63 p. – Текст : непосредственный.

8.4.2 Japanese patent №: JP 6001562 B2, IPC G06F 3/01 (2006.01), G06F 3/0481 (2013.01). Use of 3D environmental models in game play: Appl. No.: 314015767: 09.09.2016: Publication: 05.10.2016 / Shahram Izadi, David Molyneaux, Otmar Hilliges, David Kim; Assignee: Canon Corporation. – 30 p. – Текст : непосредственный.

**8.5 Китай**

8.5.1 Chinease patent №: CN105631773B, IPC G05D 1/00(2006 .01), G06F 3/14(2006 .01), G06T 19/00(2011 .01). Electronic device and method for providing map service: Appl. No.: 201510824702.6: 24.11.2015: Publication: 19.02.2021 / Kyung-Tae Kim, Shin-Jun Lee, Eun-Seon Noh, Sun-Kee Lee, Cheol-Ho Cheong, Hyung-Jin Park, Yo-Han Lee, Dong-Soo Han; Assignee: Samsung Electronics Co Ltd. – 62 p. – Текст : непосредственный.

8.5.2 Chinease patent №: CN105144238B, IPC G03D 35/02 (2006 .01). 3D imaging methods and system: Appl. No.: 201480022819.6: 25.02.2014: Publication: 11.02.2018 / Peiman Mugadam; Assignee: Commonwealth Scientific and Industrial Research Organization CSIRO. – 33 p. – Текст : непосредственный.

**9 Сводный библиографический список литературы**

1. Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. – 136 c. – Текст : непосредственный.

2. Коржик, В. И. Основы криптографии: монография / В. И. Коржик, В.А. Яковлев. – Санкт-Петербург: Интермедия, 2016 – 296 с. – Текст : непосредственный.

3. Goldreich, O. Foundations of Cryptography: A Primer : монография / O. Goldreich. – Almaty : Al-Farabi Kazakh National University Press, 2005. – 132 p. – Текст : непосредственный.

4. Lynn M.. Elliptic Curve Cryptography: монография / M. Lynn – Cambridge : Cambridge University Press, 2013. – 102 p. – Текст: непосредственный.

5. Смирнова, М. А. Асимметричное шифрование как способ проверки подлинности автора сообщения / М. А. Смирнова, И. А. Самойлова, Л. В. Устинова– Текст : непосредственный //Актуальные проблемы современности. – 2017. – № 2. – 5 с.

6. Умрзоков, С. Криптографические протоколы / С. Умрзоков – Текст : непосредственный // Мировая наука. – 2029. – № 6. – 5 с.

7. Xiaojuan Chen. Analysis of Cryptographic Protocol by Dynamic Epistemic Logic / Xiaojuan Chen, Huiwen Deng – Текст : непосредственный // IEEE. – 2019. – № 7. – 7 p.

8. Krishna Chaitanya Nunna. Secure Data Transfer Through Internet Using Cryptography and Image Steganography / Krishna Chaitanya Nunna – Текст : непосредственный // IEEE. – 2017. – №.12 – 7 p.

9. Сизоненко, А. Б. Модели и алгоритмы синтеза логико-вычислительных подсистем защиты информации систем критического применения : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Сизоненко Александр Борисович; Воронежский институт МВД РФ. – Воронеж, 2016. – 310 с. – Текст: непосредственный.

10. Новиков, С. Н. Методология зашиты информации на основе технологий сетевого уровня мультисервисных сетей связи : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Новиков Сергей Николаевич; Томский государственный университет систем управления и радиоэлектроники. – Томск, 2016. – 235с. – Текст: непосредственный.

11. Evmorfia-Iro Bartzia. A formalization of elliptic curves for cryptography. Doctoral dissertation / Evmorfia-Iro Bartzia; Université Paris Saclay. – 2017. – 127 p. – Текст : непосредственный.

12. Karpman, Pierre. Analysis of symmetric primitives. Doctoral dissertation / P. Karpman; Nanyang Technological University. – 2016. – 103 p. – Текст: непосредственный.

13. Назаров, Н. И. Алгоритмы криптографии, использующие генераторы случайных или псевдослучайных чисел / Н. И. Назаров; Самарский государственный технический университет. – Самара, 2011. – 9 с. – Деп. в НТИЦ ГА от 31.08.2011 № 401-В2011. – Текст : непосредственный.

14. Бенсон, Я. Е. Моделирование динамических процессов / Я. Е. Бенсон, Е. Г. Зудов; Уральский государственный технический университет. – Екатеринбург, 2007. – 65 с. – Деп в ВИНИТИ РАН от 26.04.2007 № 1100-B2007 – Текст : непосредственный.

15. Мазунина, Е. С. Сквозное шифрование / Е. С. Мазунина. – Текст : непосредственный // Научное сообщество студентов. – 2016. – С. 48-50.

16. Казанцев, А.А. Криптография и криптоанализ / А. А. Казанцев. – Текст : непосредственный // Школьная секция: информационные технологии. – 2019. – C. 18.

17. Peng, Sheng-Lung. Proceedings of First International Conference on Mathematical Modeling and Computational Science / Sheng-Lung Peng, Hao, Rong-Xia, Pal, Souvik. – Текст : непосредственный // ICMMCS. – 2020.

18. Escalante, S. Automatic Recognition of Peruvian Car License Plates / S. Escalante, V. Murray. – Текст : непосредственный // Proceedings of the 2020 IEEE 27th International Conference on Electronics, Electrical Engineering and Computing, INTERCON. – 2020.

19. Математические алгоритмы криптографии / В.В. Меньших; руководитель НИОКТР к.т.н. Меньших В. В. // отчет о НИОКР, рег. номер: 07170612. – 2017. – 10с.

20. Основы информационной безопасности и защиты информации в ОВД / С.В. Крыгин, С.Н. Сухов, Т.Е. Чикина, А.О. Логинов; руководитель НИОКТР доктор физико-математических наук Крыгин С.В // отчет о НИОКР, рег. номер: 07170919; План научной деятельности на 2017 год Нижегородской академии МВД России; «Нижегородская академия МВД России». – 2017. – 129 с.

21. Патент № 2544737 Российская Федерация, МПК RU 2520379 C2 (06.05.2021). Криптография на эллиптической кривой: № 2021616056/08 : заявл. 22.04.2021 : опубл. 06.05.2021 / Икар Тома, Корон Жан-Себастьен; заявитель Электро Грундлер (RU). – 17 с. : ил. – Текст : непосредственный.

22. Патент № 2617972 Российская Федерация, МПК RU 2016617549 A (20.06.2016. Криптографическое шифрование: № 2016108116 : заявл. 18.05.2016 : опубл. 07.07.2016 / Насыров Ринат Ришатович, Сулейманов Игорь Рашидович, Чуркин Андрей Игоревич.; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (RU). – 2 с. : ил. – Текст : непосредственный.

23. United States Patent №: US 2017/0161614 A1, IPC G06N 5/02 (2006.01), G06F 7/50 (2006.01). Systems and methods for predicting emergency situations: Appl. No.: 15/371,117 : 6.12.2016 : Publication: 8.06.2017 / Anil Mehta, Michael John Martin, Nicholas Edward Horelik ; Assignee: Rapidsos Inc. (US). – 46 p. – Текст : непосредственный.

24. United States Patent №: US 2021/0186329 A1, IPC A61B 5/00 ( 2006.01 ), A61B 8/00 ( 2006.01 ), H04M 3/51 ( 2006.01 ), GO8B 21/04 ( 2006.01 ), G16H 50/20 ( 2006.01 ), G16H 15/00 ( 2006.01 ), G16Z 99/00 ( 2006.01 ), A61B 7700 ( 2006.01 ), A61B 5/318 ( 2006.01 ), A61B ( 2006.01 ), 5/369 ( 2006.01 ), A61B 5/389 ( 2006.01 ), A61B 5/01 ( 2006.01 ), A61B 5/0205 ( 2006.01 ). Mesh network personal emergency response appliance: Appl. No.: 17/177,282 : 17.02.2021: Publication: 24.06.2021 / Bao Tran(US); Assignee: KONINKLIJKE PHILIPS. – 77 p. – Текст : непосредственный.

25. European patent №: EP 2494525B1, IPC G06T 15/00 (2011.01), G03B 35/16 (2006.01), G06T 15/04 (2011.01). A method for automatic material classification and texture simulation for 3d models: Appl. No.: 14754127.0: 25.02.2014: Publication: 10.06.2020 / Peyman Moghadam; Assignee: Commonwealth Scientific and Industrial Research Organization CSIRO. – 30 p. – Текст : непосредственный.

26. European patent №: EP 2959459B1, IPC G06T 15/04 (2011.01) G06T 17/05 (2011.01). 3d-abbildungsverfahren und -system: Appl. No.: 10828764.0: 18.10.2010: Publication: 05.02.2020 / Stephen Schultz; Assignee: Pictometry International Corp. – 22 p. – Текст : непосредственный.

27. Japanese patent №: JP 5933632 B2, IPC G06F 3/0481 (2013.01), G05B 23/02 (2006.01). Graphic elements with multiple visualizations in a process environment: Appl. No.: 512132022: 13.05.2013: Publication: 15.06.2016 / Kyoomi Yamazawa, Kikuo Matsuzawa; Assignee: Seiko Instr & Electronics Ltd. – 63 p. – Текст : непосредственный.

28. Japanese patent №: JP 6001562 B2, IPC G06F 3/01 (2006.01), G06F 3/0481 (2013.01). Use of 3D environmental models in game play: Appl. No.: 314015767: 09.09.2016: Publication: 05.10.2016 / Shahram Izadi, David Molyneaux, Otmar Hilliges, David Kim; Assignee: Canon Corporation. – 30 p. – Текст : непосредственный.

29. Chinease patent №: CN105631773B, IPC G05D 1/00(2006 .01), G06F 3/14(2006 .01), G06T 19/00(2011 .01). Electronic device and method for providing map service: Appl. No.: 201510824702.6: 24.11.2015: Publication: 19.02.2021 / Kyung-Tae Kim, Shin-Jun Lee, Eun-Seon Noh, Sun-Kee Lee, Cheol-Ho Cheong, Hyung-Jin Park, Yo-Han Lee, Dong-Soo Han; Assignee: Samsung Electronics Co Ltd. – 62 p. – Текст : непосредственный.

30. Chinease patent №: CN105144238B, IPC G03D 35/02 (2006 .01). 3D imaging methods and system: Appl. No.: 201480022819.6: 25.02.2014: Publication: 11.02.2018 / Peiman Mugadam; Assignee: Commonwealth Scientific and Industrial Research Organization CSIRO. – 33 p. – Текст : непосредственный.

**Выводы**

1. В ходе практической работы, патентов и публикаций было найдено в колличестве 30 штуки по теме исследований “ Разработка программы моделирования передачи сообщений с асимметричным и симметричным шифрованием данных”:

– монографий: 4;

– статей: 4;

– диссертаций: 4;

– депонированных рукописей: 2;

– публикаций в материалах НТК: 4;

– отчетов о НИР: 2;

– патентов: 10.

2. Найденная информация по теме исследования является:

– адекватной, вследствие того, что информация , создаваемая с помощью предметов исследования, таких как статьи, монографии, патенты и т.д., соотвествует реальному объекту, процессу и определяет степень соответствия образа объекта самому объекту, так называемая семантическая адекватность;

– репрезентативной, так как выборка производится из разных журналов, статей и конференций, что позволяет повысить ее репрезентативность;

– достаточной, поскольку она содержит минимальный, но достаточный для принятия правильного решения состав, так как отражает часть проблем,таких как моделирование процессов передачи сообщений;

– доступной, потому что получена из открытых источников

– актуальной, так как существует достаточное количество статей, публикаций, книг, патентов и диссертаций по теме исследования за последние пять – десять лет;

– своевременной, поскольку данная информация может быть использована в научной работе для решения узконаправленных проблем, например, симуляция передачи данных;

– достоверной, потому что получена из официальных источников;

– устойчивой, так как полученная информация остается актуальной в течение относительно длительного периода времени (по меньшей мере, годы).