БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Рабочий экземпляр №

УТВЕРЖДАЮ
Проректор по учебной работе
А. А. Сакович
5 июня 2019 г.
Регистрационный № УД-244-II_уч.

Нейрокриптографические методы защиты данных

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-40 80 02 Системный анализ, управление и обработка информации

2019 г.

Учебная программа составлена на основе образовательного стандарта высшего образования второй ступени (магистратуры) ОСВО 1-40 80 02-2019 (утвержден и введен в действие постановлением Министерства образования Республики Беларусь № 81 от 26.06.2019) и учебных планов утвержденных ректоратом БГТУ 30.05.19., рег. № 40-2-19-061/уч. (для очной (дневной) формы обучения) и № 40-2-19-062/уч. (для заочной формы обучения)

Составитель:

П. П. Урбанович, профессор кафедры информационных систем и технологий учреждения образования «Белорусский государственный технологический университет», доктор технических наук, профессор

Рецензенты:

Н.И. Белодед, доцент кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь», кандидат технических наук, доцент,

Д. М. Романенко, заведующий кафедрой информатики и веб-дизайна учреждения образования «Белорусский государственный технологический университет», кандидат технических наук, доцент.

Рекомендована к утверждению:
Кафедрой информационных систем и технологий учреждения образования «Белорусский государственный технологический университет» (протокол №12 от 13.06.2019 г.)

Учебно-методическим советом учреждения образования «Белорусский государственный технологический университет» (протокол № 7 от 28.06.2019 г.).

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Характеристика учебной дисциплины

Курс предназначен для изучения магистрантами теоретических основ и овладения ими практическими навыками совместного использования криптографических методов и нейросетевых технологий для защиты данных в компьютерных системах и сетях. Учебная программа по дисциплине «Нейрокриптографические методы защиты данных» разработана для обучающихся на второй ступени высшего образования в соответствии со стандартом и учебным планом специальности 1-40 80 02 Системный анализ, управление и обработка информации

Цели и задачи учебной дисциплины

Целью дисциплины «Нейрокриптографические методы защиты данных» является изучение и практическое освоение магистрантами методов, алгоритмов и инструментальных средств повышения информационной безопасности и надежности систем хранения, преобразования и передачи информации и защиты информации в информационно-вычислительных системах (ИВС) с использованием нейросетевых технологий и криптографии, приобретение практических навыков по созданию и использованию методов и средств повышения информационной безопасности и надежности систем.

Основные задачи изучения дисциплины:

- изучение математических основ нейросетевых технологий;
- приобретение знаний о методах и средствах повышения информационной безопасности и надежности систем хранения данных с использованием нейрокриптографии;
- получение практических навыков разработки и реализации нейрокриптографических алгоритмов с использованием языков функционального программирования.

Место учебной дисциплины в системе подготовки магистра

Учебная дисциплина входит в состав вариативного модуля «Управление данными» (компонент учреждения высшего образования) учебного плана УО БГТУ по специальности высшего образования II ступени (магистратуры) 1-40 80 02: Системный анализ, управление и обработка информации.

Изучение учебной дисциплины основывается на знаниях и умениях, приобретенных при изучении таких дисциплин как «Объектно-ориентированные технологии проектирования и программирования», «Основы дискретной математики», «Защита информации и надежность информационных систем», «Криптографические методы защиты информации», дисциплины «Основы информационных технологий» для соискателей ученой степени кандидата технических наук, является основополагающей для подготовки магистерской диссертации.

Требования к уровню освоению содержания учебной дисциплины

Изучение дисциплины обеспечивает формирование следующей специализированной компетенции:

СК 7 – обладать знаниями и навыками применения искусственных нейронных сетей в криптографических методах защиты данных.

В результате освоения учебной дисциплины «Нейрокриптографические методы защиты данных» магистрант должен

знать:

- особенности информационных вычислительных систем, как объекта защиты;
- классификацию, структуру и принципы функционирования искусственных нейронных сетей (ИНС);
- методы обучения ИНС;
- методы нейрокриптографической защиты данных;
- современные программно-технические средства преобразования и защиты данных в ИВС на основе технологий ИНС;

***уметь*:**

- разрабатывать программные средства защиты данных на основе методов нейрокриптографии;
- использовать прикладные средства защиты данных с использованием криптографии и нейросетевых технологий при решении практических задач;

***владеть*:**

- методологией проектирования и использования средств защиты данных на основе криптографии и нейросетевых технологий.

Форма получения высшего образования второй ступени – очная (дневная) и заочная.

Учебным планом специальности 1-40 80 02 Системный анализ, управление и обработка информации для изучения дисциплины «Нейрокриптографические методы защиты данных» предусмотрено всего 120 часов, в том числе:

– для очной формы получения образования: 60 часов аудиторных занятий, из них 30 часов – лекции, 30 часов – лабораторные занятия;

– для заочной формы получения образования: 22 часа аудиторных занятий, из них 10 часов – лекции, 12 часов – лабораторные занятия.

Распределение аудиторного времени по видам занятий, курсам и семестрам составляет:

Форма получения высшего образования II ступени	Форма контроля (семестр)		Объем работы (в часах)			Распределение по видам занятий		
			Всего, в том числе	из них				
	Зачет	Экзамен		аудиторных часов	самостоятельная работа	лекции	лабораторные занятия	практические / семинарские занятия
Очная (дневная)	–	2	120	60	60	30	30	-
Заочная	–	3	120	22	98	10	22	-

Форма текущей аттестации по учебной дисциплине – экзамен.

Трудоемкость учебной дисциплины – 3 зачетные единицы.

II. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Анализ проблем и методов криптографического преобразования информации.

Основные элементы криптографических систем. Симметричные криптосистемы. Асимметричные криптосистемы. Протокол обмена ключами, основанный на асимметричной криптосистеме. Другие направления применения асимметричных криптосистем. Безопасность криптографических систем. Хеш-функции. Применения хеш-функции. Хеш-функция без ключа. Хеш-функция с ключом.

Тема 2. Математические модели и обучение нейронных сетей.

Мозг человека как прообраз нейронной сети. Биологическая и математическая модели нейрона. Слой нейронов как сеть с прямой связью. Однослойные и многослойные сети. Технология нейронных сетей. Взаимодействие нейронных сетей. Обучение нейронной сети. Модель учитель-ученик. Прогнозирование и генерирование временных рядов. Взаимное обучение. Синхронизация дискретных весовых коэффициентов персептронов. Модели Хебба и анти-Хебба.

Тема 3. Использование нейронных сетей для криптографических приложений.

Архитектура нейронных сетей на основе целых действительных чисел. Модель сети Кинцеля-Кантера для согласования тайной (ключевой) информации. Анализ архитектуры сети на основе действительных чисел (TPM). Процесс синхронизации архитектур TPM на основе моделей Хебба и анти-Хебба. Безопасность процесса синхронизации архитектур TPM. Модификация метода обучения архитектуры TPM. Атаки на нейросетевые структуры на основе TPM.

Тема 4. Математические модели и архитектуры нейронных сетей на основе алгебр комплексных чисел, кватернионов и октониов.

Модель и архитектура системы нейросетевого криптопреобразования на основе комплексных чисел (TPCM) и кватернионов (TPQM). Архитектура и модель сети на основе октонионов (TPOM). Особенности архитектуры и моделей сетей.

Тема 5. Компьютерные имитационные модели функционирования и безопасность нейронных сетей.

Анализ безопасности архитектур нейронных сетей. Сравнительный анализ безопасности архитектур TPM, TPCM, TPQM, TPOM. Анализ ограничения вектора весов TPCM в контексте безопасности обмена ключами. Эффективность геометрической и других видов атак на сети. Выбор параметра окончания процесса синхронизации. Хеш-функции, основанные на нейронных сетях. Сети QNNHF (Quaternion Neural Network Hash Function). Анализ безопасности хеш-функции, основанной на архитектуре нейронной сети.

III. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Учебно-методическая карта учебной дисциплины
«Нейрокриптографические методы защиты данных» для очной формы получения образования

Номер раздела, темы занятия	Название раздела, темы занятия; перечень изучаемых вопросов	Количество аудиторных часов				Самостоятельная работа	Литература	Учебно-методическое обеспечение учебных занятий	Форма контроля знаний по учебной дисциплине
		Лекции	Практические занятия	Лабораторные занятия	Семинарские занятия				
1	2	3	4	5	6	7	8	9	10
1.	**Тема 1. Анализ проблем и методов криптографического преобразования информации** 1. Основные элементы криптографических систем. Симметричные и асимметричные криптосистемы. 2. Хеш-функции и их применение.	**2**	**-**	**4**	–	**10**	[4-5]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
2.	**Тема 2. Математические модели и обучение нейронных сетей** 1. Однослойные и многослойные сети. Технологии нейронных сетей. 2. Модели и методы обучения нейронных сетей.	**6**	**-**	**6**	–	**15**	[1, 2, 10, 11, 17-19]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
3.	**Тема 3. Использование нейронных сетей для криптографических приложений** 1. Модель Кинцеля-Кантера. 2. Процесс синхронизации архитектур TPM. 3.Безопасность процесса синхронизации архитектур TPM.	**10**	**-**	**10**	–	**15**	[6-12]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам. Коллоквиум

1	2	3	4	5	6	7	8	9	10
4.	**Тема 4. Математические модели и архитектуры нейронных сетей на основе алгебр комплексных чисел, кватернионов и октонионов** 1. Основы алгебр комплексных чисел, кватернионов и октонионов. 2. Компьютерная реализация архитектур TPCM, TPQM, TPOM.	**6**	**-**	**6**	**–**	**10**	[13-16]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
5.	**Тема 5. Компьютерные имитационные модели функционирования и безопасность нейронных сетей** 1. Сравнительный анализ безопасности архитектур TPM, TPCM, TPQM, TPOM. 2 Сети QNNHF.	**6**	**-**	**4**	**–**	**10**	[7- 9, 13-16, 20-22]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам. Коллоквиум
Всего часов по видам занятий		**30**	**-**	**30**	**–**	**60**			
Итого		**120**							
Форма итогового контроля		**Экзамен**							

3.2. Учебно-методическая карта учебной дисциплины
«Нейрокриптографические методы защиты данных» для заочной формы получения образования

Номер раздела, темы занятия	Название раздела, темы занятия; перечень изучаемых вопросов	Количество аудиторных часов				Самостоятельная работа	Литература	Учебно-методическое обеспечение учебных занятий	Форма контроля знаний по учебной дисциплине
		Лекции	Практические занятия	Лабораторные занятия	Семинарские занятия				
1	2	3	4	5	6	7	8	9	10
1.	**Тема 1. Анализ проблем и методов криптографического преобразования информации** 1. Основные элементы криптографических систем. Симметричные и асимметричные криптосистемы. 2. Хеш-функции и их применение.	**1**	**-**	**2**	–	**15**	[4-5]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
2.	**Тема 2. Математические модели и обучение нейронных сетей** 1. Однослойные и многослойные сети. Технологии нейронных сетей. 2. Модели и методы обучения нейронных сетей.	**2**	**-**	**2**	–	**15**	[1, 2, 10, 11, 17-19]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
3.	**Тема 3. Использование нейронных сетей для криптографических приложений** 1. Модель Кинцеля-Кантера. 2. Процесс синхронизации архитектур TPM. 3.Безопасность процесса синхронизации архитектур TPM.	**3**	**-**	**3**	–	**25**	[6-12]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам. Коллоквиум

1	2	3	4	5	6	7	8	9	10
4.	**Тема 4. Математические модели и архитектуры нейронных сетей на основе алгебр комплексных чисел, кватернионов и октонионов** 1. Основы алгебр комплексных чисел, кватернионов и октонионов. 2. Компьютерная реализация архитектур TPCM, TPQM, TPOM.	**2**	**-**	**3**	**–**	**23**	[13-16]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам
5.	**Тема 5. Компьютерные имитационные модели функционирования и безопасность нейронных сетей** 1. Сравнительный анализ безопасности архитектур TPM, TPCM, TPQM, TPOM. 2 Сети QNNHF.	**2**	**-**	**2**	**–**	**20**	[7- 9, 13-16, 20-22]	ЭКЛ, ЭУМК, Презентация	Обсуждение, дискуссия. Устная защита отчетов по лабораторным работам. Коллоквиум
Всего часов по видам занятий		**10**	**-**	**12**	**–**	**98**			
Итого		**120**							
Форма итогового контроля		**Экзамен**							

IV. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

4.1. Рекомендуемая литература

Основная литература:

1. Хайкин, С. Нейронные сети: полный курс, изд. 2-е: Пер. с англ./ С. Хайкин. – М.: Издательский дом “Вильямс”, 2006. – 1104 с. (Ресурсы удаленного доступа: https://diskstation.belstu.by, https://lib-bkm.ru/13779)

2. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы/ Д. Рутковская, М. Пилиньский, Л. Рутковский. – М.: Горячая линия – Телеком, 2006. – 452 с. (Ресурсы удаленного доступа: https://diskstation.belstu.by, https://yadi.sk/d/1s0aCnE0qhFiD)

3. Головко, В. А. Нейросетевые технологии обработки данных/ В.А. Головко, В.В. Краснопрошин. – Минск: БГГУ, 2017. – 263 с. (Ресурс удаленного доступа: http://elib.bsu.by/bitstream/123456789/193558/1/Golovko.pdf)

4. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П.П. Урбанович. - Минск: БГТУ, 2016. - 220 с. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/23763)

5. Урбанович, П. П. Информационная безопасность и надежность систем: учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. - Минск: БГТУ, 2007. - 87 с. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/2937)

Дополнительная литература:

6. W. Kinzel and I. Kanter. Interacting neural networks and cryptography. In B. Kramer, editor, Advances in Solid State Physics, volume 42, Springer, Berlin, 2002. – P. 383–391(Ресурс удаленного доступа: https://link.springer.com/chapter/10.1007%2F3-540-45618-X_30)

7. A. Klimov, A. Mityaguine, and A. Shamir. Analysis of neural cryptography. In Y. Zheng, editor, Advances in Cryptology—ASIACRYPT 2002, Springer, Heidelberg, 2003. – P. 228. (Ресурс удаленного доступа: https://link.springer.com/content/pdf/10.1007%2F3-540-36178-2_18.pdf)

8. Ruttor, A. Neural Synchronization and Cryptography/ A. Ruttor, Dissertation zur Erlangung des naturwissenschaftlichen Doktorgrades der Bayerischen Julius-Maximilians-Universit¨ at W¨urzburg, W¨urzburg, 2006. – 117 p. (Ресурс удаленного доступа: https://arxiv.org/pdf/0711.2411.pdf)

9. Плонковски, М. Использование нейронных сетей в операциях над хеш-функциями / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI, Физ-мат. науки и информатика. 2005. – Вып. XIII. – С. 169 – 171.

10. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Серия VI. Физико-математические науки и информатика. – Минск: БГТУ. - 2005. - Вып. XIII.- С.161-164. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/26748)

11. Плонковски, М. Использование нейронных сетей в системах криптографического преобразования информации / М. Плонковски, П. П. Урбанович // Известия Белорусской инженерной академии, 2004, № 1(17). – С. 13-15. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/26748)
12. Урбанович, П. П. Эффективность геометрической атаки на компьютерные сети / П. П. Урбанович, М. Д. Плонковски, К. В. Чуриков // Международная научно-техническая конференция "Автоматический контроль и автоматизация производственных процессов": материалы конференции, Минск, 28-29 октября 2009 г. - Минск, 2009. - С. 40-42. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/25730)
13. Plonkowski, M. Wykorzystanie kwaternionów w protokole uzgadniania klucza kryptograficznego, opartym na architekturach sieci neuronowych TPQM / M. Plonkowski, P. Urbanowicz, E. Lisica // Przeglad Elektrotechniczny. – 2010. – V. 86. – №7. – P. 90-91. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/31439)
14. Urbanovich, P. Probabilistic measure of space for neurocryptographic system solutions / P. Urbanovich, D. Karczmarski, M. Plonkowski // Proc. of 11th Intern. Conf. NEET'2019, Zakopane, Poland, June 25 - 28, 2019. – Lublin University of Techn., 2019. – P. 32. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/31444)
15. Płonkowski, M. Split-complex numbers in neural cryptography / M. Płonkowski, P. Urbanovich // 7th International Conference "New Electrical and Electronic Technologies and their Industrial Implementation" – NEET'2011, Zakopane, Poland, June 28–July 1, 2011. – P. 146. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/25716)
16. Урбанович, П. П. Моделирование и анализ процесса синхронизации нейронных сетей для обмена критической информацией / П. П. Урбанович, М. Долецки // Материалы XVII МНТК «Комплексная защита информации. Безопасность информационных технологий», 18.05.2012, Суздаль . – 2012. – С. 255-257. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/26744)
18. Урбанович, П. П. Сравнительный анализ методов взаимообучения нейронных сетей в задачах обмена конфиденциальной информацией / П. П. Урбанович, К. В. Чуриков // Труды БГТУ. Сер. VI, Физико-математические науки и информатика. - Минск: БГТУ, 2010. – Вып. XVIII. – С. 163-166. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/24402)
19. Лисица, Е. В. Моделирование криптографических систем на основе нейронных сетей / Л. В. Лисица, П. П. Урбанович // Международная научно-техническая конференция "Автоматический контроль и автоматизация производственных процессов": материалы конференции, Минск, 28-29 октября 2009 г. - Минск, 2009. - С. 79-81. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/25734)
20. Урбанович П. П., Бирюк И. А., Плонковски М. Д. Анализ синхронизации нейронных сетей в прикладной криптографии, Информационные технологии и системы 2019 (ИТС 2019): материалы международной научной конференции, БГУИР, Минск, Беларусь, 30 октября 2019 г. – Information Technologies and Systems 2019 (ITS 2019) : Proceeding of The International Conference, BSUIR,

Minsk, 30th October 2019/ редкол.: Л. Ю. Шилин [и др.]. – Минск: БГУИР, 2019, p. 278-279. (Ресурс удаленного доступа: https://libeldoc.bsuir.by/handle/123456789/37512)
21. Urbanovich, P. The appearance of conflict by using the chaos function to calculate the hash code /P. Urbanovich, M. Plonkowski, K. Churikau // 7th International Conference “New Electrical and Electronic Technologies and their Industrial Implementation” – NEET’2011, Zakopane, Poland, June 28–July 1, 2011. – P. 151. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/25719)
22. Urbanovich, P. The appearance of conflict when using the chaos function for calculating the hash code / Pavel Urbanovich, Marcin Plonkowski , Konstantsin Churikov // Przegląd elektrotechniczny. - 2012. - R. 88, № 11b. – P. 346-347. (Ресурс удаленного доступа: https://elib.belstu.by/handle/123456789/24784)

4.2. Методические рекомендации по организации и выполнению самостоятельной работы магистрантов

Изучение дисциплины «Нейрокриптографические методы защиты данных» осуществляется путем проведения лекций, лабораторных занятий, организации самостоятельной работы магистрантов, а также индивидуальной работы преподавателя с магистрантами.

Преподавание дисциплины предполагает использование современных информационных технологий для чтения лекций и проведения лабораторных занятий.

Самостоятельная работа магистранта по дисциплине включает следующие виды деятельности:

– подготовка рефератов по согласованным с преподавателем темам;

– самостоятельное изучение функционала существующих инструментальных средств на основе технологий искусственных нейронных сетей;

– выполнение отчетов по выполненным лабораторным работам;

– подготовка к аттестации по учебной дисциплине.

В рамках изучения дисциплины предусмотрено выполнение шести работ:

1. Исследование и анализ производительности существующей аппаратно-программной платформы для выполнения операций над большими числами на основе модулярной арифметики.

2. Разработка программного приложения (симулятора) для согласования ключевой информации между двумя или более абонентами по открытым компьютерным сетям

3. Программная реализация модели TPM с указанными преподавателем параметрами сетей.

4. Исследование процесса синхронизации параметров весовых коэффициентов персептронов двух сетей TPM.

5. Исследование процесса синхронизации параметров весовых коэффициентов персептронов двух сетей на основе комплексных чисел, кватернионов и октонионов.

6. Разработка приложения для вычисления хеш-функций на основе нейросетевой технологии.

4.3. Перечень рекомендуемых средств диагностики результатов учебной деятельности

Контроль качества усвоения материалов по дисциплине «Нейрокриптографические методы защиты данных» осуществляется в форме текущей аттестации магистрантов по учебной дисциплине в рамках лабораторных занятий, по итогам 2-х коллоквиумов и на экзамене.

ВОПРОСЫ К ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ
«Нейрокриптографические методы защиты данных»

1. Основные элементы криптографических систем.
2. Симметричные криптосистемы. Асимметричные криптосистемы.
3. Протокол обмена ключами, основанный на асимметричной криптосистеме. Другие направления применения асимметричных криптосистем.
4. Безопасность криптографических систем.
5. Хеш-функции. Применения хеш-функции.
6. Хеш-функция без ключа. Хеш-функция с ключом.
7. Мозг человека как прообраз нейронной сети. Биологическая и математическая модели нейрона.
8. Слой нейронов как сеть с прямой связью. Однослойные и многослойные сети.
9. Технология нейронных сетей. Взаимодействие нейронных сетей.
10. Обучение нейронной сети. Модель учитель-ученик.
11. Прогнозирование и генерирование временных рядов.
12. Взаимное обучение нейронных сетей.
13. Синхронизация дискретных весовых коэффициентов персептронов. Модели Хебба и анти-Хебба.
14. Архитектура нейронных сетей на основе целых действительных чисел.
15. Модель сети Кинцеля-Кантера для согласования тайной (ключевой) информации.
16. Анализ архитектуры сети на основе действительных чисел (TPM).
17. Процесс синхронизации архитектур TPM на основе моделей Хебба и анти-Хебба.
18. Безопасность процесса синхронизации архитектур TPM.
19. Модификация метода обучения сетей на основе архитектуры TPM.
20. Атаки на нейросетевые структуры на основе TPM.
21. Модель и архитектура системы нейросетевого криптопреобразования на основе комплексных чисел (TPCM) и кватернионов (TPQM).
22. Архитектура и модель сети на основе октонионов (TPOM). Особенности архитектуры и моделей сетей.
23. Анализ безопасности архитектур нейронных сетей.
24. Сравнительный анализ безопасности архитектур TPM, TPCM, TPQM, TPOM.
25. Анализ ограничения вектора весов TPCM в контексте безопасности обмена ключами.
26. Эффективность геометрической и других видов атак на сети. Выбор параметра окончания процесса синхронизации.
27. Хеш-функции, основанные на нейронных сетях. Сети QNNHF (Quaternion Neural Network Hash Function).
28. Анализ безопасности хеш-функции, основанной на архитектуре нейронной сети.

4.4. Требования к реферату

Для лучшего усвоения материала по дисциплине «Нейрокриптографические методы защиты данных» предусматривается подготовка каждым магистрантом 2-х рефератов, предусматривающих выполнение анализ современных нейросетевых технологий. Общий объем реферата около 10 страниц.

Структура реферата:

- титульный лист;
- содержание;
- введение (до 1страницы);
- 1-2 аналитических раздела;
- выводы (1-2 страницы);
- библиографический список.

V. ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

по дисциплине ««Нейрокриптографические методы защиты данных»»
для специальности 1-40 80 02 Системный анализ, управление и обработка информации

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Объектно-ориентированные технологии проектирования и программирования	Программной инженерии	Предложений нет	Протокол № 12 от 27.06.2019
Защита информации и надежность информационных систем, Криптографические методы защиты информации, Основы информационных технологий	Информационных систем и технологий	Предложений нет	Протокол № 12 от 13.06.2019
Основы дискретной математики	Информатики и вебдизайна, Информационных систем и технологий	Предложений нет	Протокол № 12 от 28.06.2019 Протокол № 12 от 13.06.2019

Заведующий кафедрой ИСиТ

к.т.н., доцент (подпись) **В.В. Смелов** (инициалы, фамилия)